代数中的反例

胡 崇 慧 编

陕西科学技术出版社

代数中的反例

胡崇慧　编

陕西科学技术出版社出版

（西安北大街131号）

陕西省新华书店发行　　西安新华印刷厂印刷

开本 787×1092　1/32　印张 4　字数 82,000

1983年6月第1版　　1983年6月第1次印刷

印数 1—20,000

统一书号：7202·79　　定价：0.46元

前　言

“全等的两个三角形一定是相似的”，这一命题是正确的，那么我们就要加以严格证明；“相似的两个三角形一定是全等的”这一命题是不正确的，那么我们就要找出两个相似三角形并不全等，也就是说，举一个反例。由此看来，对于命题来说，给出证明和构造反例是同样重要的。

本书的主要内容是举出关于代数中的反例，包括高等代数和近世代数基础两部分。在前一部分中，环上的线性空间一节已超出高等代数的范围，但它对理解线性空间的结构不是无益的。在举反例的过程中，所涉及到的定理、命题的论证均可在高等代数和近世代数基础中找到。为了有助于对问题的理解，我们还加入了一些说明性的例题。

本书参考了张禾瑞教授著的《近世代数基础》及由王世强教授执笔的《关于代数教材的几点注记》的讲义等材料。

在编写过程中，张德荣同志精心审阅了全部手稿，提出许多改进意见；同时还得到我的老师和其他同志的帮助，谨此一并感谢。

希望同志们多加指正。

1982年6月

目　　录

高等代数部分

第一章　多　项　式

这一章，我们主要是讨论数域P上的一元多项式，并举出有关的反例，关于整除、最大公因式、互素、不可约、k重因式以及本原多项式这一系列的概念，都为大家所熟悉，就不一一叙述了。

下面就举一些相关的反例。

1.　如果$f(x)|g_i(x)$，$i=1, 2, \cdots, n$，那么$f(x)$就能整除$g_1(x)$，$g_2(x)$，$\cdots$，$g_n(x)$的组合，即

$$f(x)|(u_1(x)g_1(x)+u_2(x)g_2(x)+\cdots+u_n(x)g_n(x))$$

反之不真。即$f(x)$能整除$g_1(x)$，$g_2(x)$，$\cdots$，$g_n(x)$的组合，未必$f(x)|$每一个$g_i(x)$。

例　$$f(x)=3x-2$$

而　$$g_1(x)=x^2+1,\qquad g_2(x)=2x+3$$

$$u_1(x)=-2,\qquad u_2(x)=x$$

显然　$$f(x)|(u_1(x)g_1(x)+u_2(x)g_2(x))$$

但　$$f(x)\nmid g_i(x)$$

2.　$P[x]$中的多项式$f(x)$与$g(x)$的最大公因式是$d(x)$，那么有$P[x]$中多项式$u(x)$与$v(x)$使

$$d(x)=u(x)(f(x)+v(x)g(x)$$

但 i） **反之不真**。即上式成立，$d(x)$ 未必是 $f(x)$ 与 $g(x)$ 的最大公因式；

ii） **满足上式的$u(x)$与$v(x)$不是唯一的**。

例 i） $f(x)=x$， $g(x)=x+1$

有 $$x(x+2)+(x+1)(x-1)=2x^2+2x-1$$

其中 $u(x)=x+2$， $v(x)=x-1$

而 $2x^2+2x-1$显然不是$f(x)$与$g(x)$的最大公因式。

我们说，当

$$d(x)=u(x)f(x)+v(x)g(x)$$

而$d(x)$是$f(x)$与$g(x)$的一个公因式时，$d(x)$一定是 $f(x)$ 与 $g(x)$的一个最大公因式。

例ii） $f(x)=x^2-1$， $g(x)=1$

则$d(x)=1$

$$\begin{cases}u(x)=-1\\ v(x)=x^2\end{cases}$$

$$\begin{cases}u(x)=0\\ v(x)=1\end{cases}$$

$$\begin{cases}u(x)=-2\\ v(x)=2x^2-1\end{cases}$$

3. 多项式$f_1(x)$，$f_2(x)$，…，$f_n(x)$（$n>2$）互素时，并不一定两两互素。

例i） $f_1(x)=x^2-3x+2$

$$f_2(x)=x^2-5x+6$$

$$f_3(x)=x^2-4x+3$$

是互素的，但

$$(f_1(x),\ f_2(x)) = x-2$$

例ii) $f_1(x) = x^3 - 7x^2 + 7x + 15$

$$f_2(x) = x^2 - x - 20$$

$$f_3(x) = x^3 + x^2 - 12x$$

则 $(f_1(x),\ f_2(x),\ f_3(x)) = 1$

而 $(f_1(x), f_2(x)) = x - 5$

$$(f_1(x), f_3(x)) = x - 3$$

$$(f_2(x), f_3(x)) = x + 4$$

4. 不可约多项式 $p(x) | f(x)g(x)$ 则有 $p(x) | f(x)$ 或 $p(x) | g(x)$。

我们说，$p(x)$是不可约多项式的限制是必要的，否则，即可举出以下**反例**：

令 $p(x) = (x-1)^2$，$f(x) = x-1$，$g(x) = x-1$

显然有 $p(x) | f(x)g(x)$，但$p(x) \nmid f(x)$及$p(x) \nmid g(x)$

5. 若不可约多项式$p(x)$是$f(x)$的k重因式（$k \geq 1$），则 $p(x)$是 $f'(x)$的 $k-1$ 重因式。

反之不真。举例如下：

令 $f(x) = x^3 - 3x^2 + 3x - 3$

则 $f'(x) = 3x^2 - 6x + 3$

$x-1$是$f'(x)$ 的 2 重因式，但 $x-1$ 不是$f(x)$ 的 3 重因式，其实，就不是$f(x)$的因式。

6. 本原多项式不一定是不可约的。

例 $x^2 + 3x + 2$ 是本原的，可是

$$x^2 + 3x + 2 = (x+1)(x+2)$$

7. 设$f(x)$，$g(x)$是整系数多项式，且$g(x)$是本原的，若$f(x) = g(x)h(x)$，其中 $h(x)$ 是有理系数多项式，则 $h(x)$

一定是整系数的。

我们说，$g(x)$限制为本原的条件不可缺少，否则就有

$$f(x)=x^2+x,\qquad g(x)=2x+2$$

而 $$f(x)=g(x)h(x)$$

那么 $$h(x)=\frac{1}{2}x$$

8. *Eisenstein* 判别法告诉我们：

当 $$f(x)=a_nx^n+a_{n-1}x^{n-1}+\cdots+a_0$$

是一个整系数多项式，存在一个素数p使得

i） $p\nmid a_n$；

ii） $p|a_i$，$i=0$，1，…，$n-1$；

iii） $p^2\nmid a_0$。

那么$f(x)$在有理数域上是不可约的。

可是当找不到这样的素数p，我们不能判定其是否可约。

例 $f_1(x)=x^2+3x+2$

$f_2(x)=x^2+1$

对$f_1(x)$及$f_2(x)$来说，找不到满足判别法条件的素数p，但$f_1(x)$可约，$f_2(x)$不可约。

9. $f(x)$在有理数域上可约，它不一定有有理根。

例 $$f(x)=(x^2+1)^2$$

这一章的最后，给出关于多项式函数的反例。

定义 如果在多项式$f(x)$与$g(x)$中，同次项的系数全相等，那么$f(x)$与$g(x)$就叫做**相等**，记为

$$f(x)=g(x)$$

定义 由一个多项式定义的函数称为数域P上的**多项式函数**。

即设　　$f(x)=a_0x^n+a_1x^{n-1}+\cdots+a_n$

是$P[x]$中的多项式，α是P中的数，在$f(x)$的表达式中用α代x所得的数

$$a_0\alpha^n+a_1\alpha^{n-1}+\cdots+a_n.$$

称为$f(x)$当$x=\alpha$时的值，记为$f(\alpha)$。这样一来，多项式$f(x)$就定义了一个数域P上的函数。

我们知道，两个多项式相等必然导出两个多项式函数相等；

反之，两个多项式函数相等是否必然导出两个多项式相等呢？

当P是数域时，回答是肯定的，其原因是数域中有无穷多个数。

当P是有穷多个元素时，回答是未必。

例　Z_2是以2为模的剩余类环。

考察Z_2上多项式

$$f(x)=x+1$$

与

$$g(x)=x^2+1$$

$$f(0)=g(0)=1$$

$$f(1)=g(1)=0$$

所以，这里的两个多项式函数$f(x)$与$g(x)$相等，但是，这里的两个多项式$f(x)$与$g(x)$不等。

第二章　矩　　阵

矩阵乘法

定义　设$A=(a_{ij})mn$，$B=(b_{ij})np$
那么矩阵　$C=(c_{ij})mp$
其中

$$c_{ij}=a_{i1}b_{1j}+a_{i2}b_{2j}+\cdots+a_{in}b_{nj}=\sum_{k=1}^{n}a_{ik}b_{kj}$$

称为A与B的乘积，记为

$$C=AB$$

注意，两个矩阵只有当第一个矩阵的列数等于第二个矩阵的行数时才能相乘。

矩阵乘法不适合交换律。

i）　$A_{mn}B_{np}$有意义，当$m\neq p$时，$B_{np}A_{mn}$没有意义。如$A_{43}B_{35}$有意义，而$B_{35}A_{43}$没有意义。

ii）　$A_{mn}B_{nm}$与$B_{nm}A_{mn}$都有意义，当$m\neq n$时，它们阶数不等，如$A_{43}B_{34}$是4阶的，$B_{34}A_{43}$是3阶的。

iii）　$A_{nn}B_{nn}$与$B_{nn}A_{nn}$的阶数都是n，也不一定相等。

例　$A=\begin{pmatrix}1 & 2\\ 2 & 1\end{pmatrix}$，　$B=\begin{pmatrix}2 & -3\\ 3 & 1\end{pmatrix}$

$$AB=\begin{pmatrix}8 & -1\\ 7 & -5\end{pmatrix},\quad BA=\begin{pmatrix}-4 & 1\\ 5 & 7\end{pmatrix}$$

有关矩阵乘法的例题

1.存在零因子

即 $A \neq O$, $B \neq O$ 而有 $AB = O$。

例 $A = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$, $B = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}$

但 $AB = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$

一般说来，有

$$A_{n\times n} = \begin{pmatrix} 1 & 0 & 0 & \cdots & 0 \\ 0 & 0 & 0 & \cdots & 0 \\ 0 & 0 & 0 & \cdots & 0 \\ \cdots & \cdots & \cdots & \cdots & 0 \\ 0 & 0 & 0 & \cdots & 0 \end{pmatrix}$$

$$B_{n\times n} = \begin{pmatrix} 0 & 0 & 0 & \cdots & 0 \\ 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & 0 & \cdots & 0 \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ 0 & 0 & 0 & \cdots & 0 \end{pmatrix}$$

$$AB = \begin{pmatrix} 0 & 0 & 0 & \cdots & 0 \\ 0 & 0 & 0 & \cdots & 0 \\ 0 & 0 & 0 & \cdots & 0 \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ 0 & 0 & 0 & \cdots & 0 \end{pmatrix}$$

又如

$$A=\begin{pmatrix}1 & -1\\ -1 & 1\\ 1 & -1\end{pmatrix},\qquad B=\begin{pmatrix}1 & 2\\ 1 & 2\end{pmatrix}$$

而 $$AB=\begin{pmatrix}1 & -1\\ -1 & 1\\ 1 & -1\end{pmatrix}\begin{pmatrix}1 & 2\\ 1 & 2\end{pmatrix}=\begin{pmatrix}0 & 0\\ 0 & 0\\ 0 & 0\end{pmatrix}$$

2. 上例中同阶矩阵相乘的情形里，$A\neq O$，$B\neq O$而有$AB=O$，同时有$BA=O$。

现举一例是$A\neq O$，$B\neq O$而有$AB=O$，而$BA\neq O$。

例 $$A=\begin{pmatrix}1 & 1\\ 0 & 0\end{pmatrix},\qquad B=\begin{pmatrix}1 & 1\\ -1 & -1\end{pmatrix}$$

那么 $$AB=\begin{pmatrix}0 & 0\\ 0 & 0\end{pmatrix}$$

而 $$BA=\begin{pmatrix}1 & 1\\ -1 & -1\end{pmatrix}$$

和上例一样，可以举出同样结论的n阶阵的例。

3. 乘法消去律不成立。

$A\neq O$，$AB=AC$未必有$B=C$

例 $$A=\begin{pmatrix}1 & 1\\ -1 & -1\end{pmatrix},$$

$$B=\begin{pmatrix}1 & -1\\ -1 & 1\end{pmatrix},\qquad C=\begin{pmatrix}-1 & 1\\ 1 & -1\end{pmatrix}$$

显然，$A\neq O$，$AB=AC$，而$B\neq C$

4. 一般说来

$$(AB)^k\neq A^kB^k$$

例

$$A=\begin{pmatrix}2 & 1\\ 3 & 2\end{pmatrix},\qquad B=\begin{pmatrix}1 & -1\\ 1 & 1\end{pmatrix}$$

$$AB=\begin{pmatrix}3 & -1\\ 5 & -1\end{pmatrix},\qquad (AB)^2=\begin{pmatrix}4 & -2\\ 10 & -4\end{pmatrix}$$

$$A^2=\begin{pmatrix}7 & 4\\ 12 & 7\end{pmatrix},\qquad B^2=\begin{pmatrix}0 & -2\\ 2 & 0\end{pmatrix}$$

$$A^2B^2=\begin{pmatrix}8 & -14\\ 14 & -24\end{pmatrix}$$

所以

$$(AB)^2\neq A^2B^2$$

n 阶阵的例只要令

$$A=\begin{pmatrix}2 & 1 & & & \\ 3 & 2 & & & \\ & & 1 & & \\ & & & \ddots & \\ & & & & 1\end{pmatrix},\qquad B=\begin{pmatrix}1 & -1 & & & \\ 1 & 1 & & & \\ & & 1 & & \\ & & & \ddots & \\ & & & & 1\end{pmatrix}$$

可知

$$(AB)^k\neq A^kB^k$$

明显地，只要$AB=BA$，就有$(AB)^k=A^kB^k$。

在这一章以下的各例中，凡是遇到只举二阶矩阵的情形，都可以类似地扩展到 n 阶矩阵的情形：将所举的二阶矩阵放入要扩展的 n 阶矩阵的左上角，再将 $n-2$ 阶的单位矩阵放置右下角，其他位置均为零。凡此，我们就不再将扩展的 n 阶矩阵一一列举了。

5. 我们知道 $(AB)'=B'A'$，可是未必有 $(AB)'=$

$A'B'$.

例 仍取

$$A=\begin{pmatrix}2 & 1\\ 3 & 2\end{pmatrix},\qquad B=\begin{pmatrix}1 & -1\\ 1 & 1\end{pmatrix}$$

而 $$A'=\begin{pmatrix}2 & 3\\ 1 & 2\end{pmatrix},\qquad B'=\begin{pmatrix}1 & 1\\ -1 & 1\end{pmatrix}$$

$$AB=\begin{pmatrix}3 & -1\\ 5 & -1\end{pmatrix},\qquad A'B'=\begin{pmatrix}-1 & 5\\ -1 & 3\end{pmatrix}$$

故有 $$(AB)'\neq A'B'$$

6. $(AB)^{-1}=B^{-1}A^{-1}$，但未必有

$$(AB)^{-1}=A^{-1}B^{-1}$$

例

$$A=\begin{pmatrix}2 & 1\\ 3 & 2\end{pmatrix},\qquad B=\begin{pmatrix}1 & -1\\ 1 & 1\end{pmatrix}$$

而

$$A^{-1}=\begin{pmatrix}2 & -1\\ -3 & 2\end{pmatrix},\qquad B^{-1}=\begin{pmatrix}\frac{1}{2} & \frac{1}{2}\\ -\frac{1}{2} & \frac{1}{2}\end{pmatrix}$$

$$AB=\begin{pmatrix}3 & -1\\ 5 & -1\end{pmatrix},\qquad (AB)^{-1}=\begin{pmatrix}-\frac{1}{2} & \frac{1}{2}\\ -\frac{5}{2} & \frac{3}{2}\end{pmatrix}$$

$$A^{-1}B^{-1}=\begin{pmatrix} \frac{3}{2} & \frac{1}{2} \\ -\frac{5}{2} & -\frac{1}{2} \end{pmatrix}$$

故有 $(AB)^{-1}\neq A^{-1}B^{-1}$

7. 不存在 n 阶矩阵A、B适合关系

$$AB-BA=E$$

可存在线性变换**A**、**B**适合关系

$$\mathbf{AB}-\mathbf{BA}=\mathbf{E}$$

请参看线性变换的有关例题。

8. 一般说来，对 n 阶矩阵A和B，等式

$$|A+B|=|A|+|B|$$

不成立。

例 n 阶矩阵

$$A=\begin{pmatrix} 1 & & & \\ & \ddots & & \\ & & 1 & \\ & & & 0 \end{pmatrix},\quad B=\begin{pmatrix} 0 & & & \\ & \ddots & & \\ & & 0 & \\ & & & 1 \end{pmatrix}$$

显然 $A+B=E$ 而 $|A+B|=|E|=1$

又 $|A|+|B|=0+0=0$

9. n 阶矩阵A、B，且$A^2=E$，$B^2=E$，未必有$(AB)^2=E$。

例如当 $n=2$ 时，

$$A=\begin{pmatrix} 1 & 2 \\ 0 & -1 \end{pmatrix}\qquad B=\begin{pmatrix} 1 & 3 \\ 0 & -1 \end{pmatrix}$$

有 $$A^2=E,\ B^2=E$$

$$AB=\begin{pmatrix}1 & 1\\ 0 & 1\end{pmatrix}$$

而 $$(AB)^m=\begin{pmatrix}1 & m\\ 0 & 1\end{pmatrix} \quad (m\text{为正整数})$$

所以 $$(AB)^m\neq E$$

特别地 $$(AB)^2\neq E$$

10. 已知有理数域Q上 3 阶矩阵

$$A=\begin{pmatrix}2 & 0 & 0\\ -3 & 1 & \frac{3}{2}\\ 2 & \frac{2}{3} & 1\end{pmatrix}$$

的行列式是 0，找一个Q上的非零 3 阶矩阵B使

$$AB=BA=O, \qquad (O\text{为零矩阵})$$

这样的B是不是唯一的？

根据条件$AB=BA=O$，找到

$$B=\begin{pmatrix}0 & 0 & 0\\ -\frac{9}{2}k & -\frac{3}{2}k & \frac{9}{4}k\\ 3k & k & -\frac{3}{2}k\end{pmatrix}$$

$$k\neq 0, \qquad k\in Q$$

确实 $$AB=BA=O$$

取 k 的不同值，就得到不同的 B。

（实）对称阵

1. 对称阵之和仍为对称阵；但对称阵之积未必是对称阵。

例

$$A=\begin{pmatrix}1 & 3\\ 3 & 2\end{pmatrix},\qquad B=\begin{pmatrix}2 & 1\\ 1 & 1\end{pmatrix}$$

而 $\quad AB=\begin{pmatrix}5 & 4\\ 8 & 5\end{pmatrix}\quad$ 不是对称阵。

应当注意的是1阶对称阵之积仍为对称阵。

2. 设A是（实）对称阵，如果$A^2=O$，就有$A=O$。

我们说，A是对称阵的条件不容忽视。

例 $\quad A=\begin{pmatrix}a & a\\ -a & -a\end{pmatrix},\quad$ （a是任意实数）

显然 $\quad A^2=O$

当$a\neq 0$时，$A\neq O$。此时，A不是对称阵。

n阶阵的情况，可令

$$A=\begin{pmatrix}a & a & & & \\ -a & -a & & & \\ & & 0 & & \\ & & & \ddots & \\ & & & & 0\end{pmatrix}$$

同样有

$$A^2=O,\qquad 而A\neq O$$

3. 实对称阵的特征值都是实数，但特征值都是实数的实矩阵未必对称。

例　$A=\begin{pmatrix}4 & 4\\1 & 4\end{pmatrix}$

的特征值为 2 和 6 ，但A不对称。

4.　实对称阵和对角阵相似。但是和对角阵相似的矩阵未必对称。

例　$A=\begin{pmatrix}1 & 0\\0 & 2\end{pmatrix}$，　$B=\begin{pmatrix}1 & -\frac{1}{2}\\0 & 2\end{pmatrix}$

$$T=\begin{pmatrix}2 & 1\\0 & 3\end{pmatrix},\quad T^{-1}=\begin{pmatrix}\frac{1}{2} & -\frac{1}{6}\\0 & \frac{1}{3}\end{pmatrix}$$

有
$$B=T^{-1}AT$$
即A与B相似，A是对角阵，而B不是对称阵。

5.　n 阶实对称阵有 n 个线性无关的特征向量。反之，有 n 个线性无关的特征向量不一定是实对称阵。

例　$A=\begin{pmatrix}4 & 6 & 0\\-3 & -5 & 0\\-3 & -6 & 1\end{pmatrix}$

A的特征值为 -2 和 1 。

属于 -2 的特征向量是（-1，1，1），属于 1 的特征向量是（-2，1，0）、（0，0，1）。这三个特征向量线性无关。但A不是对称阵。

反对称阵

所谓反对称矩阵，即要求符合条件
$$A=-A'$$

1. 关于反对称阵之积

当 阶数为 2 时，

$$A=\begin{pmatrix}0 & a\\ -a & 0\end{pmatrix},\qquad B=\begin{pmatrix}0 & -b\\ b & 0\end{pmatrix}$$

均为反对称阵。

而

$$AB=\begin{pmatrix}ab & 0\\ 0 & ab\end{pmatrix}$$

当 $a\neq 0$ 且 $b\neq 0$ 时，AB 是对称阵，且为对角形阵，亦为纯量矩阵，不是反对称阵。

我们不能将这一结论推广到 n 阶阵

例 1

$$A=\begin{pmatrix}0 & -1 & -2\\ 1 & 0 & -3\\ 2 & 3 & 0\end{pmatrix}$$

$$B=\begin{pmatrix}0 & -4 & -5\\ 4 & 0 & -6\\ 5 & 6 & 0\end{pmatrix}$$

$$AB=\begin{pmatrix}-14 & -12 & 6\\ -15 & -22 & -5\\ 12 & -8 & -28\end{pmatrix}$$

AB 既不是对称阵也不是反对称阵。

例 2

$$A=\begin{pmatrix} 0 & 0 & 2 & 0 \\ 0 & 0 & 3 & 0 \\ -2 & -3 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}$$

$$B=\begin{pmatrix} 0 & 0 & -3 & 0 \\ 0 & 0 & -1 & 0 \\ 3 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}$$

都是反对称阵，而

$$AB=\begin{pmatrix} 6 & 2 & 0 & 0 \\ 9 & 3 & 0 & 0 \\ 0 & 0 & 9 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}$$

既不是对称阵也不是反对称阵。

当然可以把以上两个例题推广到一般 n 阶阵上去。

同样，不宜忽略 1 阶的情形：

$$A=(0), \qquad B=(0)$$

$$AB=(0)$$

既可谓对称阵亦可谓反对称阵。

2. A 是 n 阶阵，当 A 是对称阵时，A^n 仍为对称阵；

当 A 是反对称阵时：A^m 是反对称阵，当 m 是奇数时；A^m 是对称阵，当 m 是偶数时。

3. 不存在奇数阶的可逆反对称阵。也就是说，奇数阶的反对称阵的行列式为 0 。

而偶数阶的反对称阵的行列式不一定为0。

例

$$A=\begin{pmatrix}0 & -1 & 0 & 0\\ 1 & 0 & 0 & 0\\ 0 & 0 & 0 & -1\\ 0 & 0 & 1 & 0\end{pmatrix}$$

显然 $|A|\neq 0$

当然偶数阶的反对称阵的行列式亦可为0。

例

$$A=\begin{pmatrix}0 & -1 & 0 & 0\\ 1 & 0 & 0 & 0\\ 0 & 0 & 0 & 0\\ 0 & 0 & 0 & 0\end{pmatrix}$$

显然 $|A|=0$

但是也有一个必然结论的情况，那就是2阶非零的反对称阵的行列式一定不为0。

例 $A=\begin{pmatrix}0 & a\\ -a & 0\end{pmatrix}$ 而 $a\neq 0$

而 $|A|=a^2\neq 0$ 当 $a\neq 0$ 时。

正 定 阵

1. 正定阵的和还是正定阵，但正定阵的差未必是正定阵。

例 $A=\begin{pmatrix}1 & 1\\ 1 & 2\end{pmatrix}$, $B=\begin{pmatrix}1 & -1\\ -1 & 2\end{pmatrix}$

都是正定阵，但

$$A-B=\begin{pmatrix}0 & 2\\ 2 & 0\end{pmatrix}$$

不是正定阵。

2. 正定阵的积未必是正定阵。

例 1 $A=\begin{pmatrix}1 & 1\\ 1 & 2\end{pmatrix}$, $B=\begin{pmatrix}1 & -1\\ -1 & 2\end{pmatrix}$

而

$$AB=\begin{pmatrix}0 & 1\\ -1 & 3\end{pmatrix}$$

不是正定阵。

例 2 $A=\begin{pmatrix}1 & 2\\ 2 & 5\end{pmatrix}$, $B=\begin{pmatrix}1 & -1\\ -1 & 2\end{pmatrix}$

都是正定阵。

而

$$AB=\begin{pmatrix}-1 & 3\\ -3 & 8\end{pmatrix}$$

不是正定阵。

还应指出的是，在 1 阶阵中：

若 $A=(a)$，$B=(b)$ 都是正定阵。则其乘积

$$AB=(ab)$$

也是正定阵。

3. A是正定阵则A的行列式$|A|>0$。

但对称阵B的行列式$|B|>0$，B未必是正定阵。

例

$$B=\begin{pmatrix}1 & & \\ & -1 & \\ & & -1\end{pmatrix}$$

而 $|B|=1>0$，但 B 不是正定阵。

4. A是正定阵则 A 的主对角线上元素都大于零。

但反之不真。

例

$$A=\begin{pmatrix}1 & 3\\ 3 & 2\end{pmatrix},\qquad B=\begin{pmatrix}1 & 2\\ 2 & 4\end{pmatrix}$$

都不是正定阵。

正　交　阵

所谓正交阵指的是 n 阶实数矩阵A满足条件 $A'A=E$。

我们知道，正交阵之积仍为正交阵，那么正交阵之和是不是正交阵？

例　以下两个 n 阶阵

$$A=\begin{pmatrix}1 & & & & & \\ & -1 & & & & \\ & & 1 & & & \\ & & & 1 & & \\ & & & & \ddots & \\ & & & & & 1\end{pmatrix},\qquad B=\begin{pmatrix}1 & & & & & \\ & -1 & & & & \\ & & -1 & & & \\ & & & 1 & & \\ & & & & \ddots & \\ & & & & & 1\end{pmatrix}$$

都是正交阵。这是因为，

$$A'A=E,\qquad B'B=E$$

但

$$A+B=\begin{pmatrix}2 & & & & & \\ & -2 & & & & \\ & & 0 & & & \\ & & & 2 & & \\ & & & & \ddots & \\ & & & & & 2\end{pmatrix}$$

而

$$(A+B)'(A+B)=\begin{pmatrix}4 & & & & & \\ & 4 & & & & \\ & & 0 & & & \\ & & & 4 & & \\ & & & & \ddots & \\ & & & & & 4\end{pmatrix}\neq E$$

所以，正交阵的和不是正交阵。

另一个问题是：

若A是正交阵，则$|A| = \pm 1$，但**反之不真**。

例

$$A = \begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix}$$

而

$$|A| = 1$$

$$A'A = \begin{pmatrix} 2 & 3 \\ 3 & 5 \end{pmatrix} \neq E.$$

$$B = \begin{pmatrix} 1 & 1 \\ -1 & -2 \end{pmatrix}$$

而

$$|B| = -1$$

$$B'B = \begin{pmatrix} 2 & 3 \\ 3 & 5 \end{pmatrix} \neq E$$

即A、B都不是正交阵。

等价矩阵、合同矩阵、相似矩阵

1. 合同矩阵一定是等价矩阵，但**反之不真**。

例 取

$$B = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \qquad A = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

$$P = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \qquad Q = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$$

显然有 $B = PAQ$

即A与B等价，但A与B不合同，否则

$$\begin{aligned} B &= C'AC \\ &= C'C \end{aligned}$$

令 $$C' = \begin{pmatrix} a & b \\ c & d \end{pmatrix}, \qquad C = \begin{pmatrix} a & c \\ b & d \end{pmatrix}$$

而 $$C'C = \begin{pmatrix} a^2 + b^2 & ac + bd \\ ac + bd & c^2 + d^2 \end{pmatrix} = B$$

就有 $ac + bd = 1$， $ac + bd = 0$， 故矛盾。

2. 相似矩阵一定是等价矩阵，但反之不真。

例 仍取 $B = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$， $A = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$

知A与B等价，但A与B不相似，否则

$$B = T^{-1}AT = T^{-1}T = E$$

故矛盾。

3. 相似矩阵未必合同。

例 $$A = \begin{pmatrix} 1 & 0 \\ 0 & 2 \end{pmatrix}, \qquad B = \begin{pmatrix} 1 & -\frac{1}{2} \\ 0 & 2 \end{pmatrix}$$

$$T = \begin{pmatrix} 2 & 1 \\ 0 & 3 \end{pmatrix}, \qquad T^{-1} = \begin{pmatrix} \frac{1}{2} & -\frac{1}{6} \\ 0 & \frac{1}{3} \end{pmatrix}$$

那么 $$B = T^{-1}AT$$

即A与B相似，但A与B不合同，否则

$$\begin{aligned} B &= C'AC \\ &= \begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} 1 & 0 \\ 0 & 2 \end{pmatrix}\begin{pmatrix} a & c \\ b & d \end{pmatrix} \\ &= \begin{pmatrix} a^2 + 2b^2 & ac + 2bd \\ ac + 2bd & c^2 + 2d^2 \end{pmatrix} \end{aligned}$$

$$ac+2bd=-\frac{1}{2}$$

$$ac+2bd=0$$

故矛盾。

4. 合同矩阵未必相似。

例 取

$$B=\begin{pmatrix}1 & 0\\ 0 & 4\end{pmatrix},\qquad A=\begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix}$$

$$C=\begin{pmatrix}1 & 0\\ 0 & 2\end{pmatrix},\qquad C'=\begin{pmatrix}1 & 0\\ 0 & 2\end{pmatrix}$$

则 $$B=C'AC$$

即A与B合同，但A与B不相似，否则

$$B=T^{-1}AT=T^{-1}T=E$$

故矛盾。

5. A可逆，则有AB与BA相似，**反之不真。**

例 $A=\begin{pmatrix}1 & 0\\ 0 & 0\end{pmatrix}$，$B=\begin{pmatrix}2 & 0\\ 0 & 0\end{pmatrix}$

显然有AB与BA相似，而A没有逆.

6. 相似矩阵有相同的特征多项式，但**反之不真。**

例 $A=\begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix}$，$\qquad B=\begin{pmatrix}1 & 1\\ 0 & 1\end{pmatrix}$

$$|\lambda E-A|=(\lambda-1)^2,\ |\lambda E-B|=(\lambda-1)^2$$

即有相同特征多项式，可是A与B不相似。

7. $B=T^{-1}AT$，$B=Q^{-1}AQ$，而T未必就等于Q。

例 $A=\begin{pmatrix}1 & 1\\ 0 & 1\end{pmatrix}$, $B=\begin{pmatrix}1 & 1\\ 0 & 1\end{pmatrix}$

$T=\begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix}$, $Q=\begin{pmatrix}2 & 0\\ 0 & 2\end{pmatrix}$

则有 $B=T^{-1}AT$, $B=Q^{-1}AQ$

而 $T\neq Q$

第三章　线性空间

§1　线性空间

1.　定义　V是一个非空集合，F是一个数域，V有一个加法，F、V间有一个数乘；它们满足以下条件，V就叫做F上的一个**线性空间**。

加法满足下面四条规则：

1）$\alpha+\beta=\beta+\alpha$；

2）$(\alpha+\beta)+\gamma=\alpha+(\beta+\gamma)$；

3）在V中有一个元素0，对$\forall\alpha\in V$有

$$\alpha+0=\alpha;$$

4）对$\forall\alpha\in V$，都$\exists\beta\in V$使

$$\alpha+\beta=0;$$

数乘满足下列两条规则：

5）$1\alpha=\alpha$；$(\forall\alpha\in V)$

6）$k(l\alpha)=(kl)\alpha$；

数乘与加法满足下面两条规则：

7）$(k+l)\alpha=k\alpha+l\alpha$；

8）$k(\alpha+\beta)=k\alpha+k\beta$。

（其中，$\forall k,\ l\in F$；$\forall\alpha,\beta,\gamma\in V$）

根据这一定义，易证1）是其他七条的必然结果，这只

要计算

$$(1+1)(\alpha+\beta)=(1+1)\alpha+(1+1)\beta=\alpha+(\alpha+\beta)+\beta$$

以及

$$(1+1)(\alpha+\beta)=1(\alpha+\beta)+1(\alpha+\beta)=\alpha+(\beta+\alpha)+\beta$$

则可以证得

$$\alpha+\beta=\beta+\alpha$$

但是其他七条即2）—8）是独立的，我们给出线性空间的与之等价的另一定义。

2. 等价定义

V是一个非空集合，F是一个数域，V有一个加法，F，V间有一个数乘，它们满足以下条件，V就叫做F上的一个**线性空间**。

加法满足下面三条规则：

A）$\alpha+\beta=\beta+\alpha$；

B）$(\alpha+\beta)+\gamma=\alpha+(\beta+\gamma)$；

C）方程

$$\alpha+x=\beta$$

在V中可解；

数乘满足下面两条规则：

D）$1\alpha=\alpha$，$(\forall\alpha\in V)$

E）$k(l\alpha)=(kl)\alpha$；

数乘与加法满足下面两条规则：

F）$(k+l)\alpha=k\alpha+l\alpha$；

G）$k(\alpha+\beta)=k\alpha+k\beta$。

（其中，$\forall k$，$l\in F$，$\forall\alpha$，β，$\gamma\in V$）

上述两个定义的等价性容易证明，我们的着眼点是给出

$A)$—$G)$ 是独立的例。

例1 F是数域，$V=\{$所有正有理数$\}$。

加法：$\alpha+\beta=\beta$

数乘：$k\alpha=\alpha$

容易验证$B)$—$G)$ 都被满足，只有$A)$ 不被满足：

$$2+3=3$$

而 $$3+2=2$$

例2 $B)$ 是独立的。

F 是数域，$V=\{o,\alpha,\beta,\gamma\}$。

加法

	o	α	β	γ
o	o	α	β	γ
α	α	α	o	α
β	β	o	β	α
γ	γ	α	α	γ

数乘 $k\alpha=\alpha$

可知 $(\alpha+\beta)+\gamma=\gamma\neq\alpha=\alpha+(\beta+\gamma)$

但其余各条均成立。

例3 $C)$ 是独立的。

F 是数域，$V=\{o,\ \alpha,\ \beta\}$。

加法

	o	α	β
o	o	α	α
α	α	α	α
β	α	α	β

数乘　　$k\alpha=\alpha$

我们说，方程

$$\alpha+x=\beta$$

在V中无解，其他条件可以验证成立。

例4. D）是独立的。

F是数域，$V=\{$所有实数$\}$。

普通加法，数乘，$k\alpha=0$

显然不满足　$1\alpha=\alpha$

而其他各条均成立。

例5. E）是独立的。

$F=\left\{a+b\sqrt{2}\ \middle|\ a,\ b\text{有理数}\right\}$，　　$V=\left\{\text{全体有理数}\right\}$。

加法是普通数的加法，

数乘：$(a+b\sqrt{2})\alpha=(a+b)\alpha$

由　　$(\sqrt{2}\sqrt{2})1=(2)1=2$

$\sqrt{2}(\sqrt{2}\cdot 1)=\sqrt{2}\cdot 1=1$

知不满足　　$(kl)\alpha=k(l\alpha)$

但其余各条均成立。

例6. F）是独立的。

F是实数域，$V=\{$所有实数$\}$。

普通加法，数乘：$k\alpha=\alpha$

易知不满足　　$(k+l)\alpha=k\alpha+l\alpha$

而其他各条均成立。

例7. G）是独立的。

F是实数域，$V=\{$全体非零实数$\}$。

加法　　$\alpha+\beta=\alpha\beta$，数乘，普通乘法。

由 $$2(1+1)=2(1\cdot 1)=2$$

$$2\cdot 1+2\cdot 1=2+2=4$$

知不满足 $k(\alpha+\beta)=k\alpha+k\beta$

但其他各条均成立。

3.是不是每一个加群都能作成域上的线性空间？

这里说的加群，就是一个非空集合V，它的加法，满足线性空间定义中的1）—4）。这里说的域不一定是数域。

一个加群能否作成域上的线性空间，数乘起着重要作用，但也有这样的可能，即不管怎样规定数乘，都作不成线性空间。

例　V为整数加群，Z_p是以素数p为模的剩余类环，当然是域。

我们说，V作不成Z_p上的线性空间。

由假设知道，Z_p的特征为p。

即 $$\underbrace{1+1+\cdots+1}_{p\text{个}}=0$$

$2\in V$，$1\in Z_p$，若V能作成Z_p上线性空间，则应满足5)：$1\alpha=\alpha$。由此，则应

$$1\circ 2=2$$

还应满足 $$0\circ\alpha=0$$

那么 $$0=0\circ 2=(\underbrace{1+1+\cdots+1}_{p\text{个}})\circ 2$$

$$=(1\circ 2)+\cdots+(1\circ 2)$$

$$=2+\cdots+2$$

$=2p$

但在整数加群V里$2p\neq 0$。

这就是说，无论怎样规定数乘，V 都不能作成 Z_p 上的线性空间。

§ 2　线性相关性

1. 定义　设α_1，$\alpha_2,\cdots,\alpha_r$是线性空间V的 r 个向量，若在F中存在不全为零的数 $k_1,k_2\cdots$，k_r，使得

$$k_1\alpha_1+k_2\alpha_2+\cdots+k_r\alpha_r=0$$

则说向量α_1，$\alpha_2,\cdots,\alpha_r$**线性相关**。

2.　β不能由α_1，$\alpha_2,\cdots,\alpha_r$线性表示，$\beta,\alpha_1,\cdots\alpha_r$是否一定线性无关？

例　$\beta=(1,1,1,),\alpha_1=(1,0,0)$，$\alpha_2=(2,0,0)$

明显地是β不能由α_1，α_2线性表示，然而

$$\beta,\ \alpha_1,\ \alpha_2$$

线性相关。

这个例题同时说明，如果α_1，α_2，$\cdots$，α_r线性相关，未必其中每一个向量都是其余向量的线性组合。

3.　若α_1，$\alpha_2,\cdots,\alpha_r$线性无关，则其中任意两个不同的向量必定线性无关，反之如何？即两两线性无关，是否全部线性无关？

例　$\alpha_1=(1,1,1)$，$\alpha_2=(0,1,0)$，$\alpha_3=(1,0,1)$

这里任意两个向量都线性无关。

可是　　$\alpha_1=\alpha_2+\alpha_3$

即α_1，α_2，α_3线性相关。

4. 设α_1，α_2，α_3线性无关，则$\alpha_1+\alpha_2$，$\alpha_2+\alpha_3$，$\alpha_3+\alpha_1$也线性无关。

我们说，若α_1，α_2，α_3，α_4线性无关，$\alpha_1+\alpha_2$，$\alpha_2+\alpha_3$，$\alpha_3+\alpha_4$，$\alpha_4+\alpha_1$是否也线性无关呢？

回答是一定线性相关，也就是说，不管α_1，α_2，α_3，α_4是不是线性无关，$\alpha_1+\alpha_2$，$\alpha_2+\alpha_3$，$\alpha_3+\alpha_4$，$\alpha_4+\alpha_1$必定线性相关。

还可以将这些结论推广到m个的情形。

当$\alpha_1, \alpha_2, \cdots, \alpha_m$（$m$是奇数）线性无关时，$\alpha_1+\alpha_2$，$\alpha_2+\alpha_3$，$\cdots, \alpha_{m-1}+\alpha_m$，$\alpha_m+\alpha_1$也线性无关。

事实上，若

$$k_1(\alpha_1+\alpha_2)+k_2(\alpha_2+\alpha_3)+\cdots+k_{m-1}(\alpha_{m-1}+\alpha_m)+k_m(\alpha_m+\alpha_1)=0$$

有 $$(k_1+k_m)\alpha_1+(k_2+k_1)\alpha_2+(k_3+k_2)\alpha_3+\cdots+(k_m+k_{m-1})\alpha_m=0$$

由于 $\alpha_1, \alpha_2, \cdots, \alpha_m$线性无关，

所以
$$\begin{aligned} k_1 \qquad\qquad\qquad +k_m &= 0 \\ k_1+k_2 \qquad\qquad\qquad &= 0 \\ k_2+k_3 \qquad\qquad &= 0 \\ \cdots\cdots\cdots\cdots\cdots\cdots \\ k_{m-1}+k_m &= 0 \end{aligned}$$

$$D=\begin{vmatrix} 1 & 0 & 0 & 0 & \cdots & 0 & 1 \\ 1 & 1 & 0 & 0 & \cdots & 0 & 0 \\ 0 & 1 & 1 & 0 & \cdots & 0 & 0 \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\ 0 & 0 & 0 & 0 & \cdots & 1 & 1 \end{vmatrix}$$ 按第一行展开

$$
=\begin{vmatrix} 1 & 0 & 0 & \cdots & 0 & 0 \\ 1 & 1 & 0 & \cdots & 0 & 0 \\ 0 & 1 & 1 & \cdots & 0 & 0 \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\ 0 & 0 & 0 & \cdots & 1 & 1 \end{vmatrix} + (-1)^{1+m} \begin{vmatrix} 1 & 1 & 0 & 0 & \cdots & 0 \\ 0 & 1 & 1 & 0 & \cdots & 0 \\ 0 & 0 & 1 & 1 & \cdots & 0 \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\ 0 & 0 & 0 & 0 & \cdots & 1 \end{vmatrix}
$$

$= 2$ （因为m是奇数）

$\neq 0$

只有零解，即只有

$$k_1 = k_2 = \cdots = k_m = 0$$

故　　$\alpha_1+\alpha_2$，$\alpha_2+\alpha_3,\cdots,\alpha_m+\alpha_1$线性无关。

另一个结论是$\alpha_1,\alpha_2,\cdots,\alpha_m$是$m$个向量，当$m$是偶数时，$\alpha_1+\alpha_2$，$\alpha_2+\alpha_3,\cdots,\alpha_m+\alpha_1$一定线性相关，这只要看

$$(\alpha_1+\alpha_2)-(\alpha_2+\alpha_3)+\cdots+(-1)^{m+1}(\alpha_m+\alpha_1)=0$$

则显见。

§3　子　空　间

1．定义

1）子空间的定义　数域F上线性空间V的一个非空子集S叫做V的一个**子空间**，假如对V的加法及其数乘S也作成线性空间。

2）子空间的和　S_1，S_2是V的子空间，S_1与S_2的**和**是指$\{\alpha_1+\alpha_2 | \alpha_1\in S_1,\ \alpha_2\in S_2\}$，记作$S_1+S_2$。

3）子空间的直和　子空间的和S_1+S_2叫做**直和**，假如S_1+S_2中任一个向量α都表示为

$$\alpha=\alpha_1+\alpha_2 \qquad \alpha_i\in S_i \qquad (i=1,2)$$

且表示法是唯一的。

2. 子空间的直和都是和，而子空间的和未必是直和。

例 $V=\{(a_1,a_2,a_3)\mid a_i$是实数$\}$，$F$是实数域。

$S_1=\{(a_1,a_2,0)\mid a_i$ 是实数$\}$，$S_2=\{(0,b_2,b_3)\mid b_i$ 是 实数$\}$。

显然 $V=S_1+S_2$

$\forall(x,y,z)\in V$

$$(x,y,z)=(x,y,0)+(0,0,z)$$
$$=(x,0,0)+(0,y,z)$$

只要$y\neq 0$，就是两种不同的表示法。

所以 V_1+V_2 不是直和。

3. 设V是数域F上线性空间，$S_1,S_2,\cdots S_n(n\geqslant 4)$是$V$的子空间，适合

$$S_i\cap(S_j+S_k)=0 \qquad (i\neq j,k)$$

问$S_1,S_2,\cdots,S_n$的和 $S_1+S_2+\cdots+S_n$ 是否一定是直和 $S_1\dotplus S_2\dotplus\cdots\dotplus S_n$？

我们说，未必。

例 F是实数域，

$$V=\{(x_1,x_2,x_3)\mid x_i\in F\}$$

令 $S_1=L[(1,0,0)]$，$S_2=L[(0,1,0)]$

$S_3=L[(0,0,1)]$，$S_4=L[(-1,-1,-1)]$

易知 $S_i\cap(S_j+S_k)=0 \qquad (i\neq j,k)$

显然 $S_1+S_2+S_3+S_4$不是直和。

因为 $(1,0,0)+(0,1,0)+(0,0,1)+(-1,-1,-1)$
$$=(0,0,0)$$

§ 4 环上的线性空间

在数域F上的线性空间，维数是唯一的，而且子空间的维数不超过原线性空间的维数，也就是说，有限维空间的子空间是有限的，这些结论在将数域F换为环R后就不是必然的了。我们将用一些例子说明。

1. 定义

以下的环R均指有单位元的环。

1）**环上的线性空间** 一个加群V叫做环R上的一个左线性空间，若是对RV到V的数乘使得

$$1\alpha=\alpha$$
$$k(l\alpha)=(kl)\alpha$$
$$(k+l)\alpha=k\alpha+l\alpha$$
$$k(\alpha+\beta)=k\alpha+k\beta$$

这里$\forall k, l\in R$，$\forall\alpha, \beta\in V$。

2）**循环空间** R上的线性空间V叫做由向量α所生成的循环空间，假如V刚好包含所有$k\alpha(k\in R)$，以$R\alpha=\{$所有$k\alpha\mid k\in R\}$表示。

α叫做一个生成元。

3）**有限空间** 一个环R上的一个线性空间V叫做R上的一个有限空间，假如V是n个循环子空间$R\alpha_1$，$R\alpha_2,\cdots$，$R\alpha_n$的和。

4）**有基底空间** 若环R上的一个线性空间V是n个循环空间$R\alpha_1, R\alpha_2,\cdots, R\alpha_n$的直和，向量$\alpha_1,\alpha_2,\cdots,\alpha_n$叫做$V$的一个基底，$V$叫做一个有基底空间。

5) 自由空间 环R上的线性空间V叫做一个自由空间。若V是n个循环空间 $R\alpha_1, R\alpha_2, \cdots, R\alpha_n$的直和，并且0是每一个$\alpha_i$的唯一的零化子，这时$\alpha_1, \alpha_2, \cdots, \alpha_n$叫做$V$的一个自由基底，$n$叫做这个自由基底的长度，以$Vn(R)$表示。

所谓零化子指的是，R的k叫做向量α的一个零化子，假如

$$k\alpha = 0$$

2. 整数加群不能作成Z_p上的线性空间。

例 参看本章§1之3的例。

3. 子空间和的元表示法不唯一。

例 R是整数环Z，V是整数环Z。

V可以看成R上的线性空间，而$S_1=(4)$，$S_2=(6)$都是V的子空间。$10 \in S_1 + S_2$。

$$\begin{aligned} 10 &= 4 + 6 \\ &= 16 + (-6) \end{aligned}$$

4. 有限空间未必是有基底空间。

有基底空间显然是有限空间，但有限空间未必是有基底空间。

例 $Z[x]$是整数环Z上多项式环。

理想子环$(2, x)$是$Z[x]$上的一个有限空间，生成元是$2, x$。

我们说$(2, x)$不是有基底空间。

证 若$(2, x)$有一个基底$f_1(x), f_2(x), \cdots, f_n(x)$，在这些$f_i(x)$中至多有一个$\neq 0$。

否则，可假定$f_1(x) \neq 0$，$f_2(x) \neq 0$

$$0 \neq f_1(x) f_2(x) \in Z[x] f_1(x)$$

$$0 \neq -f_1(x)f_2(x) \in Z[x]f_2(x)$$

$$0 = f_1(x)f_2(x) + [-f_1(x)f_2(x)] + 0 + \cdots + 0$$

这说明 $Z[x]f_1(x) + Z[x]f_2(x) + \cdots + Z[x]f_n(x)$ 不是直和。

既然在 $f_i(x)$ 中，最多只有一个 $\neq 0$，那么 $(2, x)$ 是由一个元生成的，即 $(2, x)$ 是 $Z[x]$ 的一个主理想子环，但已经知道 $(2, x)$ 不是一个主理想子环，因而 $(2, x)$ 不能有基底。

5. 有基底空间未必是自由空间。

自由空间显然是有基底空间，可是有基底空间未必是自由空间。

例 $V = Z_p$（p素数），R 是整数环Z，规定数乘：

$$k\alpha = \alpha\text{的}k\text{倍}, \quad k \in R, \quad \alpha \in V = Z_p$$

则V是R上的有基底空间：

$$V = R1, \qquad \text{而 } 1 \text{ 是基底}$$

但 1 的零化左理想子环是 (p) 而$p \neq 0$，所以V不是自由空间。

6. 有长度不同的自由基底。

我们举一个关于环R上自由空间的自由基底有不同长度的例题。

例 F是域。

R = {所有 F上每行每列只有有限多个元 $\neq 0$ 的无限矩阵}，R是环，且有单位元。

$$E = \begin{pmatrix} 1 & & \\ & 1 & \\ & & \ddots \end{pmatrix}$$

令$V=R$

$$K_1=\begin{pmatrix}1&0&0&0&0&\cdots\\0&0&0&0&0&\cdots\\0&1&0&0&0&\cdots\\0&0&0&0&0&\cdots\\0&0&1&0&0&\cdots\\\cdot&\cdot&\cdot&\cdot&\cdot&\cdots\end{pmatrix}$$

$$K_2=\begin{pmatrix}0&0&0&0&0&\cdots\\1&0&0&0&0&\cdots\\0&0&0&0&0&\cdots\\0&1&0&0&0&\cdots\\0&0&0&0&0&\cdots\\\cdot&\cdot&\cdot&\cdot&\cdot&\cdots\end{pmatrix}$$

看

$$(K_1,\ K_2)\begin{pmatrix}K_1'\\K_2'\end{pmatrix}$$

$$=K_1K_1'+K_2K_2'$$

$$=\begin{pmatrix}1&0&0&0&0&\cdots\\0&0&0&0&0&\cdots\\0&0&1&0&0&\cdots\\0&0&0&0&0&\cdots\\0&0&0&0&1&\cdots\\\cdot&\cdot&\cdot&\cdot&\cdot&\cdots\end{pmatrix}+\begin{pmatrix}0&0&0&0&0&\cdots\\0&1&0&0&0&\cdots\\0&0&0&0&0&\cdots\\0&0&0&1&0&\cdots\\0&0&0&0&0&\cdots\\\cdot&\cdot&\cdot&\cdot&\cdot&\cdots\end{pmatrix}$$

$$=E$$

$$\begin{pmatrix} K_1' \\ K_2' \end{pmatrix}(K_1, K_2) = \begin{pmatrix} K_1'K_1 & K_1'K_2 \\ K_2'K_1 & K_2'K_2 \end{pmatrix}$$
$$= \begin{pmatrix} E & O \\ O & E \end{pmatrix}$$

这说明$\begin{pmatrix} K_1' \\ K_2' \end{pmatrix}$有逆。

$V(R)$ 以E为自由基底，长度为1；

又 $$\begin{pmatrix} \alpha_1 \\ \alpha_2 \end{pmatrix} = \begin{pmatrix} K_1' \\ K_2' \end{pmatrix} E$$

由于E是自由基底，且$\begin{pmatrix} K_1' \\ K_2' \end{pmatrix}$可逆，

所以 $\alpha_1 = K_1'E = K_1'$，$\alpha_2 = K_2'E = K_2'$亦为$V(R)$的自由基底，长度为2。

7. 自由空间与其子空间的基底长度相等的例

例 R是整数环Z，V是R上自由空间，α_1，α_2，…，α_n是V的自由基底，故其长度为n，而S是由$2\alpha_1$，$2\alpha_2$，…，$2\alpha_n$生成的子空间，易见S的长度也是n。

8. 环R上有限空间的子空间是无限空间的例

例 F是域。

$R = \{F$上无限多不定元$x_1, x_2, \cdots$之多项式$\}$

即多项式环$R = F[x_1] \cup F[x_1, x_2] \cup F[x_1, x_2, x_3] \cup \cdots$

令 $V = R$

则V为R上有限空间，1为自由基底。

$S = \{V$中0多项式及所有不含常数项的多项式$\}$

S显然是V的子空间，但不是R上的有限空间。

不然的话，设其生成元为α_1，$\alpha_2,\cdots,\alpha_n$：

$$\alpha_1 = f_1(x_{11},\ x_{12},\cdots,x_{1i_1})$$
$$\alpha_2 = f_2(x_{21},\ x_{22},\cdots,x_{2i_2})$$
$$\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots$$
$$\alpha_n = f_n(x_{n1},\ x_{n2}\cdots x_{ni_n})$$

取 $x_k \in S$

而令 $x_k \neq x_{11},\cdots,x_{1i_1},\cdots,x_{n1},\cdots,x_{ni_n}$

我们说，x_k不可能由α_1，$\alpha_2,\cdots,\alpha_n$线性表出。

若 $x_k = g_1\alpha_1 + \cdots + g_n\alpha_n \qquad (g_1,\cdots,g_n \in R)$

$$= g_1 f_1 + \cdots + g_n f_n$$

因为f_i不出现x_k，又不出现非零常数，因此，每一个$g_i f_i$均不出现$Cx_k(C\neq 0)$。这就是说，S不可能是有限空间。

9． 自由空间的子空间是无限空间的例

例 适当的环R的一个左理想子环A，A看成R上无限空间，我们找R上的自由空间$V(V\neq R)$，它有无限子空间。

$V = \{(k_1,\ k_2)\mid k_i \in R\}$

$S = \{(a,\ 0)\mid a \in A\}$

V是R上自由空间，S是V的子空间。

我们说S是V的无限子空间，否则，S有生成元α_1，α_2，$\cdots$，α_n，其中$\alpha_i = (a_i,\ 0)$。

任一$(x,0)\in S$。则有

$$(x,\ 0) = l_1\alpha_1 + l_2\alpha_2 + \cdots + l_n\alpha_n \qquad (l_i \in R)$$
$$= (l_1a_1,0) + (l_2a_2,0) + \cdots + (l_na_n,0)$$
$$= (l_1a_1 + l_2a_2 + \cdots + l_na_n,\ 0)$$

所以 $x = l_1a_1 + l_2a_2 + \cdots + l_na_n$

这就是说，A 中任一元 x 均可经由A中 $a_1, a_2, \cdots, a_n$ 线性表示，这样，就有

$$A = Ra_1 + Ra_2 + \cdots + Ra_n$$

与A是R的无限空间矛盾。

10． 自由空间的子空间不是自由空间的例

例 取R是有零因子的环：

$R = Z_n$，n是偶数即$n = 2m$，那么

$$Z_n = \{[0], [1], \cdots, [n-1]\}$$

令 $V = Z_n$ 而

$$S = \{[0], [2], \cdots, [n-2]\}$$

则有V是Z_n的自由空间。

S是V的子空间，但不是自由空间。

这是因为S的生成元$[2]$的零化子不只是$[0]$，

$$[2][m] = [2m] = [n] = [0]$$

具体地说，

$V = Z_6$是Z_6上的自由空间。

而 $S = \{[0], [2], [4]\}$是V的子空间。

S生成元$[2]$有非$[0]$零化子：

$$[2][3] = [6] = [0]$$

11． 交换环R上的左线性空间V在数乘

$$ak = ka$$

之下是R上的右线性空间。

但是当R是非交换环时，在数乘

$$ak = ka$$

之下，R上左线性空间就未必能作成R上的右线性空间。

例 Z_2是以 2 为模的剩余类环。

$$R=\left\{\begin{pmatrix} a & 0 \\ b & c \end{pmatrix} \middle| a,b,c\in Z_2\right\}$$

则R共有8个元素：

$$\begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ 1 & 1 \end{pmatrix}$$

$$\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$$

R是有单位元的环。

但R不是交换环。

$$\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}\begin{pmatrix} 1 & 0 \\ 1 & 0 \end{pmatrix}=\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$$

$$\begin{pmatrix} 1 & 0 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}=\begin{pmatrix} 1 & 0 \\ 1 & 0 \end{pmatrix}$$

令 $V=\left\{\begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix} \middle| a_{ij}\in Z_2\right\}$

显然V是加群。

数乘是矩阵乘法，则V是R上的左线性空间，但在

$$\alpha k=k\alpha$$

之下，V不是R上的右线性空间，这是因为不满足条件

$$\alpha(kl)=(\alpha k)l。$$

取 $k=\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$, $l=\begin{pmatrix} 1 & 0 \\ 1 & 0 \end{pmatrix}$, $\alpha=\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$

$$\alpha(kl)=(kl)\alpha$$

$$= \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$$

$$(ak)l = l(ak) = l(ka)$$

$$= \begin{pmatrix} 1 & 0 \\ 1 & 0 \end{pmatrix}$$

第四章　线 性 变 换

1．线性变换

1）**定义**　线性空间V的一个变换**A**叫做**线性变换**，假如对$\forall \alpha$，$\beta\in V$和$\forall k\in F$（数域），都有

i）　$\mathbf{A}(\alpha+\beta)=\mathbf{A}(\alpha)+\mathbf{A}(\beta)$，

ii）　$\mathbf{A}(k\alpha)=k\mathbf{A}(\alpha)$。

2）非线性变换的例

例1　F是数域，

$V=\{(x_1,x_2,x_3)|\ x_i\in F\}$

令

$$\mathbf{A}(x_1,x_2,x_3)=(x_1^2,x_2+x_3,x_3^2)$$

我们说，**A**不是线性变换。

当　$\alpha=(1,2,3)$，$\beta=(1,1,1)$

$$\mathbf{A}(\alpha)=(1,5,9),\quad \mathbf{A}(\beta)=(1,2,1)$$

$$\mathbf{A}(\alpha+\beta)=\mathbf{A}(2,3,4)=(4,7,16)$$

所以　$\mathbf{A}(\alpha+\beta)\neq\mathbf{A}(\alpha)+\mathbf{A}(\beta)$

即不适合 i）

$$\mathbf{A}(k\alpha)=\mathbf{A}(k,\ 2k,\ 3k)=(k^2,\ 5k,\ 9k^2)$$

$$k\mathbf{A}(\alpha)=k(1,\ 5,\ 9)=(k,\ 5k,\ 9k)$$

当$k\neq 0$、1时，　$\mathbf{A}(k\alpha)\neq k\mathbf{A}(\alpha)$

故不适合 ii）

这就给出既不适合 i）又不适合 ii）的非线性变换的一个变换。

例2 F是实数域，

$$V=\{(a, b)\mid a, b\in F\}$$

令 $\mathbf{A}(a, b)=(a, b)$，当a，b同号或至少有一为0。

$\mathbf{A}(a, b)=(-a, -b)$，当$a$，$b$异号。

显然$\mathbf{A}$是V的一个变换。

$\mathbf{A}$适合 ii）

事实上，

当a，b同号，$\mathbf{A}(k(a, b))=\mathbf{A}(ka, kb)=(ka, kb)$

$$=k(a, b)=k\mathbf{A}(a, b)$$

当a，b异号，

而$k\neq 0$，$\mathbf{A}(k(a, b))=\mathbf{A}(ka, kb)=(-ka, -kb)$

$$=k(-a, -b)=k\mathbf{A}(a, b)$$

而$k=0$，

$$\mathbf{A}(k(a, b))=(0, 0)=k\mathbf{A}(a, b)$$

当a，b至少有一个为0，

$$\begin{aligned}\mathbf{A}(k(a, b))&=\mathbf{A}(ka, kb)\\&=(ka, kb)\\&=k(a, b)\\&=k\mathbf{A}(a, b)\end{aligned}$$

但不适合 i）

$$\mathbf{A}(-2, -3)=(-2, -3)$$

$$\mathbf{A}(-1, 4)=(1, -4)$$

$$\begin{aligned}\mathbf{A}((-2, -3)+(-1, 4))&=\mathbf{A}(-3, 1)\\&=(3, -1)\\&\neq(-2, -3)+(1, -4)\end{aligned}$$

这就是说，$\mathbf{A}$ 不是线性变换，由于不适合 i）而适合

ii，说明 i ）是独立的。

例3 把复数域看作复数域上的线性空间。

令 $\mathbf{A}(\alpha)=\overline{\alpha}$

$\mathbf{A}$ 适合 i ）

事实上，

$$\begin{aligned}\mathbf{A}(\alpha+\beta)&=\overline{\alpha+\beta}\\&=\overline{\alpha}+\overline{\beta}\\&=A(\alpha)+A(\beta)\end{aligned}$$

但 A 不适合 ii)

这时取 $\alpha=1$，$k=i$

$$\mathbf{A}(k\alpha)=-i,\qquad k\mathbf{A}(\alpha)=i$$

所以 $$\mathbf{A}(k\alpha)\neq k\mathbf{A}(\alpha)$$

这就是说，$\mathbf{A}$ 不是线性变换，由于适合 i ）而不适合 ii ），说明 ii ）是独立的。

本来，确定一个变换是不是线性变换，只要举例说明不适合哪一条，不必验证适合或不适合另一条，我们以上三例之所以将适合的和不适合的都加以验证是为了给出所有可能情形的例，而更重要的一点是着重说明线性变换定义中的两个条件是互相独立的。

3 ）线性变换与一一变换

例1 O变换是线性变换，在非零线性空间里它不是一一变换。

例2 把复数域看作复数域上的线性空间。

$$\mathbf{A}(\alpha)=\overline{\alpha}$$

是一一变换但不是线性变换，因为不适合 ii ）。

例3 恒等变换E：$\mathbf{E}(\alpha)=\alpha$。

既是线性变换又是一一变换。

4）已经知道“线性变换把线性相关的向量组变为线性相关的向量组”，但**反之不真**。

例 O变换就把线性无关的向量组变成线性相关的向量组。

5）在矩阵中，不存在n阶矩阵A，B适合关系

$$AB-BA=E$$

而在线性变换中，可存在线性变换**A**、**B**适合关系

$$\mathbf{AB}-\mathbf{BA}=\mathbf{E}$$

其中**E**是恒等变换。

例 在$F[x]$中，$\mathbf{A}f(x)=f'(x)$，$\mathbf{B}f(x)=xf(x)$

$$\begin{aligned}(\mathbf{AB}-\mathbf{BA})f(x)&=\mathbf{AB}f(x)-\mathbf{BA}f(x)\\&=\mathbf{A}(xf(x))-\mathbf{B}f'(x)\\&=f(x)+xf'(x)-xf'(x)\\&=f(x)\end{aligned}$$

所以 $\mathbf{AB}-\mathbf{BA}=\mathbf{E}$。

2。线性变换的乘法不满足交换律。

例 R是实数域，线性空间$R[x]$中，线性变换

$$\mathbf{D}(f(x))=f'(x)$$

$$\mathbf{J}(f(x))=\int_0^x f(t)dt$$

的乘积 $\mathbf{DJ}=\mathbf{E}$，而一般说来$\mathbf{JD}\neq\mathbf{E}$。

3。相似的矩阵有相同的特征多项式。

即 $A\sim B\longrightarrow|\lambda E-A|=|\lambda E-B|$

但反之不真。

例　$A=\begin{pmatrix}1 & 0\\0 & 1\end{pmatrix}$，　$B=\begin{pmatrix}1 & 1\\0 & 1\end{pmatrix}$

而　$|\lambda E-A|=(\lambda-1)^2$，　$|\lambda E-B|=(\lambda-1)^2$

但　A与B不相似，这是因为

$$X^{-1}AX=X^{-1}X=E$$

这就是说，A只能与E相似，可是$B\neq E$。

4．汉密尔顿—凯莱(Hamilton－Cayley)定理

设A是数域F上一个$n\times n$矩阵，$f(\lambda)=|\lambda E-A|$是A的特征多项式，则

$$f(A)=A^n-(a_{11}+a_{22}+\cdots+a_{nn})A^{n-1}+\cdots+(-1)^n|A|E=0$$

对这个定理我们应注意以下两点：

1）A，λ_0都是$f(x)$的根，但意义不同，特征值λ_0在扩域中，而A一般不在扩域中。实际上，$A\in F_{n\times n}$（域F上$n\times n$矩阵环）。又当$n\geqslant 2$时$F_{n\times n}$，不属于F之任何扩域（$F_{n\times n}$有零因子）。

2）在域F中$f(\lambda)$（n次）最多有n个根，在环中则不然。

例　F是有理数域Q。

$$Q_{2\times 2}\ni\begin{pmatrix}1 & a\\0 & 1\end{pmatrix}=Aa,\qquad Aa\in Q$$

每一个$\begin{pmatrix}1 & a\\0 & 1\end{pmatrix}$均适合$f(\lambda)=|\lambda E-Aa|$

$$=(\lambda-1)^2$$
$$=\lambda^2-2\lambda+1$$

即有　$f(Aa)=Aa^2-2Aa+E=0$

$\lambda^2-2\lambda+1$虽是2次的，但Aa有无限多。

5．线性变换的值域与核

1） **定义**　A是线性空间V的一个线性变换，A的全体象所作成的集合叫做A的**值域**，用AV表示。在A之下零向量的所有逆象作成的集合叫做A的**核**，用$A^{-1}(0)$表示。

2）已知

$$维AV+维A^{-1}(0)=维V$$

但AV与$A^{-1}(0)$的和并不一定是V。

例　$F[x]_n$表示数域F上所有次数不超过$n-1$的多项式及零多项式的集合。

令　$$Df(x)=f'(x)$$

D的值域是$F[x]_{n-1}$，D的核就是子空间F，

$F[x]_n$是n维的，$F[x]_{n-1}$是$n-1$维的，F是1维的。

但　$F[x]_n$不是$F[x]_{n-1}$与F的和。

原因不是直和，亦即$F[x]_{n-1}\cap F=F\neq O$。

6．不变子空间

1） **定义**　A是数域F上线性空间V的线性变换，S是V的子空间，如果$\forall\alpha\in S$都有A$\alpha\in S$，我们就说S是A的不变子空间，简称A—子空间。

2）不变子空间是对线性变换而言的。

一个线性空间的子空间对一个线性变换来说是不变子空间，但对于另一个线性变换来说，就未必是不变子空间。

例　F是数域，

$V=\{(x_1,\ x_2,\ x_3)\mid x_i\in F\}$

$A(x_1,\ x_2,\ x_3)=(2x_1-x_2,\ x_2+x_3,\ x_1)$

$B(x_1,\ x_2,\ x_3)=(0,\ x_2,\ x_3)$

易知A，B都是线性变换。

而　$BV=\{(0,\ x_2,\ x_3)\}$，$B^{-1}(0)=\{(x_1,\ 0,\ 0)\}$

容易验证　$\mathbf{B}V$、$\mathbf{B}^{-1}(0)$都是$\mathbf{B}$—子空间，但都不是$\mathbf{A}$—子空间。

事实上，取$(0, 1, 1)\in \mathbf{B}V$，

$\mathbf{A}(0, 1, 1)=(-1, 2, 0)\overline{\in}\mathbf{B}V$

取$(1, 0, 0)\in\mathbf{B}^{-1}(0)$，

$\mathbf{A}(1, 0, 0)=(2, 0, 1)\overline{\in}\mathbf{B}^{-1}(0)$

另外，再计算

$$\mathbf{AB}(x_1, x_2, x_3)=\mathbf{A}(0, x_2, x_3)$$
$$=(-x_2, x_2+x_3, 0)$$
$$\mathbf{BA}(x_1, x_2, x_3)=\mathbf{B}(2x_1-x_2, x_2+x_3, x_1)$$
$$=(0, x_2+x_3, x_1)$$

因此　　　$\mathbf{AB}\neq\mathbf{BA}$

这就又给出线性变换乘法不满足交换律的一例。

这个例题是说，$\mathbf{B}V$，$\mathbf{B}^{-1}(0)$都不是$\mathbf{A}$—子空间，是否$\mathbf{A}V$，$\mathbf{A}^{-1}(0)$也都不是$\mathbf{B}$—子空间，其实不然。因为

$$\mathbf{A}(x_1, x_2, x_3)=(2x_1-x_2, x_2+x_3, x_1)$$

不但是变换而且是满射变换：

$$\forall(y_1, y_2, y_3)\in V$$

通过
$$\begin{cases}2x_1-x_2=y_1\\ x_2+x_3=y_2\\ x_1=y_3\end{cases}$$

找到　$(y_3, -y_1+2y_3, y_2+y_1-2y_3)\in V$

而　$\mathbf{A}(y_3, -y_1+2y_3, y_2+y_1-2y_3)=(y_1, y_2, y_3)$

既然是满射还可得出是单射。

所以　$\mathbf{A}V=V$，$\mathbf{A}^{-1}(0)=O$。

这就是说，$V=\mathbf{A}V$，$O=\mathbf{A}^{-1}(0)$都是$\mathbf{B}$—子空间。

3）A，B是线性空间V的线性变换。

若$\mathbf{AB}=\mathbf{BA}$则$\mathbf{B}V$，$\mathbf{B}^{-1}(0)$都是A—子空间，同样$\mathbf{A}V$，$\mathbf{A}^{-1}(0)$也都是B—子空间，**反之不真。**

例 F是数域

$V=\{(x_1, x_2, x_3)|x_i\in F\}$

而 $\mathbf{A}(x_1, x_2, x_3)=(x_1-x_2, x_2, x_3)$

$\mathbf{B}(x_1, x_2, x_3)=(-x_1, x_2, x_3)$

都是线性变换。

易知 $\mathbf{A}V=V$，$\mathbf{A}^{-1}(0)=O$ 都是B—子空间；

$\mathbf{B}V=V$，$\mathbf{B}^{-1}(0)=O$ 都是A—子空间。

可是
$$\mathbf{AB}(x_1, x_2, x_3)=\mathbf{A}(-x_1, x_2, x_3)=(-x_1-x_2, x_2, x_3)$$
$$\mathbf{BA}(x_1, x_2, x_3)=\mathbf{B}(x_1-x_2, x_2, x_3)=(-x_1+x_2, x_2, x_3)$$

因而
$$\mathbf{AB}\neq\mathbf{BA}$$

近世代数基础部分

第五章　基本概念

§1　映射、变换

A_1，A_2，…，A_n是n个集合。D是另一个集合。

定义　若通过一个法则ϕ，对$A_1\times A_2\times\cdots\times A_n$的每一个元$(a_1, a_2, \cdots, a_n)$ $(a_i\in A_i)$，都得到唯一一个D的元d，那么这个法则ϕ叫做集合$A_1\times A_2\times\cdots\times A_n$到集合$D$的**一个映射**。

一个映射用以下符号表述

$$\phi: \quad (a_1, a_2, \cdots, a_n)\longrightarrow d=\phi(a_1, a_2, \cdots, a_n)$$

定义　$A\times B$到D的一个映射叫做$A\times B$到D的一个**代数运算**。

一个代数运算，也可以表示为

$$\circ: \quad (a, b)\longrightarrow d=a\circ b$$

定义　在集合A到集合$\overline{A}$的一个映射ϕ下，$\overline{A}$的每一个元都至少是A中某一个元的象，那么ϕ叫做A到$\overline{A}$的一个**满射**。

定义　A到$\overline{A}$的一个映射

ϕ:　$a \longrightarrow \overline{a}$

叫做A到$\overline{A}$的一个**单射**，假如

$$a \neq b \Rightarrow \overline{a} \neq \overline{b}$$

定义　若一个集合A到集合$\overline{A}$的一个映射ϕ既是满射又是单射，那么ϕ叫做A与$\overline{A}$间的一个**一一映射**。

定义　A到A的映射叫做A的一个**变换**。

A到A的满射、单射或A与A间的一一映射分别叫做A的一个**满射变换、单射变换**或**一一变换**。

1.　$A = D = \{$所有实数$\}$

ϕ:　$\begin{cases} a \longrightarrow a, & \text{若是 } a \neq 1 \\ 1 \longrightarrow b, & \text{这里 } b^2 = 1 \end{cases}$

不是A到D的一个映射，这是因为 1 的象不是唯一的。

2.　$A = D = \{$所有实数$\}$

ϕ:　$a \longrightarrow \sqrt{a}$

不是A到D的一个映射，这是因为当a是负数时，它的象不属于D。

3.　$A = \{1, 2, 3\}$

$D = \{1, 2, \cdots, 16\}$

ϕ_1:　$a \longrightarrow 2^a = \phi_1(a)$

ϕ_2:　$a \longrightarrow a^2 - a + 2 = \phi_2(a)$

易知ϕ_1和ϕ_2是A到D的两个相同的映射。

4.　$A = \{1, 2, 3, 4\}$

$D = \{1, 2, \cdots, 16\}$

ϕ_1:　$a \longrightarrow 2^a$

ϕ_2: $a \longrightarrow a^2 - a + 2$

ϕ_1和ϕ_2都是A到D的映射，但不等，这是因为

$$\phi_1(4) = 2^4 \neq 4^2 - 4 + 2 = \phi_2(4)$$

5. $A = \{1, 2, 3\}$，$\overline{A} = \{4, 5, 6, 7\}$

ϕ: $1 \to 4$，$2 \to 5$，$3 \to 6$

是单射而不是满射，故不是一一映射。

6. $A = \{1, 2, 3\}$，$\overline{A} = \{0\}$

ϕ: $a \to 0$

则ϕ是满射而不是单射，故不是一一映射。

7. A = {所有实数}

τ: $x \longrightarrow e^x$

是A的一个单射变换，不是满射变换，故不是一一变换。

8. A = {所有整数}

τ:

$$\begin{cases} a \longrightarrow \dfrac{a}{2}, & \text{若}a\text{是偶数} \\ a \longrightarrow \dfrac{a+1}{2}, & \text{若}a\text{是奇数} \end{cases}$$

是A的一个满射变换，不是单射变换，故不是一一变换。

9. A = {所有整数}，$\overline{A}$ = {所有偶数}

ϕ: $n \longrightarrow 2n$

ϕ是A与$\overline{A}$间的一一映射，而$\overline{A}$是A的真子集，不能说是A的一一变换，只不过是A的单射变换。

10. $\overline{A}$ = {所有偶数}，A = {所有整数}

ϕ: $2n \longrightarrow n$

是$\overline{A}$与A间的一一映射，而$\overline{A}$是A的真子集，不是A的变换，也不是$\overline{A}$的变换，更谈不上一一变换了。

11. $A=\{a+bw+cw^2 \mid a,\ b,\ c$为有理数，而

$$w=-\frac{1}{2}+\frac{\sqrt{3}}{2}i\}$$

$$\overline{A}=\{x+y\sqrt{2} \mid x,\ y\text{为有理数}\}$$

ϕ: $a+bw+cw^2 \longrightarrow (2a-b-c)+(b-c)\sqrt{2}$

ϕ是 A 到$\overline{A}$的一一映射。

i) 是映射

若 $a+bw+cw^2=d+ew+fw^2$

由于 $$a+bw+cw^2=a+b\left(-\frac{1}{2}+\frac{\sqrt{3}}{2}i\right)+$$

$$+c\left(-\frac{1}{2}-\frac{\sqrt{3}}{2}i\right)$$

$$=a-\frac{1}{2}(b+c)+\frac{\sqrt{3}}{2}(b-c)i$$

$$d+ew+fw^2=d-\frac{1}{2}(e+f)+\frac{\sqrt{3}}{2}(e-f)i$$

所以

$$a-\frac{1}{2}(b+c)+\frac{\sqrt{3}}{2}(b-c)i=d-\frac{1}{2}(e+f)-$$

$$-\frac{\sqrt{3}}{2}(e-f)i$$

从而

$$a-\frac{1}{2}(b+c)=d-\frac{1}{2}(e+f)$$

$$b-c=e-f$$

即 $$2a-(b+c)=2d-(e+f)$$

$$b-c=e-f$$

这样就得到

$$(2a-b-c)+(b-c)\sqrt{2}=(2d-e-f)+(e-f)\sqrt{2}$$

ii）是满射

$\forall p+q\sqrt{2}\in \overline{A}$，$\exists \frac{p+q}{2}+qw$使在$\phi$之下

$$\frac{p+q}{2}+qw+0w^2\longrightarrow p+q\sqrt{2}$$

iii）是单射

$$a+bw+cw^2\longrightarrow (2a-b-c)+(b-c)\sqrt{2}$$

$$a'+b'w+c'w^2\longrightarrow (2a'-b'-c')+(b'-c')\sqrt{2}$$

若 $(2a-b-c)+(b-c)\sqrt{2}$

$=(2a'-b'-c')+(b'-c')\sqrt{2}$

则 $2a-b-c=2a'-b'-c'$，　$b-c=b'-c'$

由此可得 $a-c=a'-c'$，$a-b=a'-b'$

那么 $a+bw+cw^2$

$=a+(a-a'+b')w+(a-a'+c')w^2$

$=(a+aw+aw^2)-a'(w+w^2)+b'w++c'w^2$

$=0-a'(-1)+b'w+c'w^2$

$=a'+b'w+c'w^2$

§2 基本算律

定义 我们说一个集合A的代数运算$\circ$（$\circ$是$A\times A$到A

的代数运算）适合**结合律**，假如对于A的任何三个元a，b，c来说，都有

$$(a\circ b)\circ c=a\circ(b\circ c)$$

定义　我们说一个$A\times A$到D的代数运算$\circ$适合**交换律**，若对于A的任何两个元a，b来说，都有

$$a\circ b=b\circ a$$

以下给分配律以定义：

$\odot$是一个$B\times A$到A的代数运算。

$\oplus$是一个A的代数运算。

定义　我们说代数运算$\odot$，$\oplus$适合**第一个（左）分配律**，若对于B的任何一个元b，A的任何两个元a_1，a_2来说，都有

$$b\odot(a_1\oplus a_2)=(b\odot a_1)\oplus(b\odot a_2)$$

第二个（右）分配律的定义完全类似。

关于结合律

1.　$A=\{$所有整数$\}$，代数运算是普通减法，我们说，它不适合结合律，因为当$c\neq 0$时

$$(a-b)-c\neq a-(b-c)$$

2.　$A=\{$所有不等于零的实数$\}$。

$\circ$是普通除法：$a\circ b=\dfrac{a}{b}$

这个代数运算不适合结合律：

$$(1\circ 1)\circ 2=\frac{1}{2},\ 1\circ(1\circ 2)=2$$

从而　$(1\circ 1)\circ 2\neq 1\circ(1\circ 2)$

3.　$A=\{$所有实数$\}$

$\circ_2$ $(a,\ b)\longrightarrow a+2b=a\circ b$

这个代数运算不适合结合律：

$(a\circ b)\circ c=a+2b+2c$，　　$a\circ(b\circ c)=a+2b+4c$

由此可知，当$c\neq 0$时，$(a\circ b)\circ c\neq a\circ(b\circ c)$

4. $A=\{$全体正整数$\}$

$a\circ b=a^b$

这个代数运算不适合结合律，这是因为

$$(2\circ 1)\circ 3=(2^1)\circ 3=(2^1)^3=2^3=8$$

$$2\circ(1\circ 3)=2\circ(1^3)=2^1=2$$

所以　$(2\circ 1)\circ 3\neq 2\circ(1\circ 3)$

5. 一个集合A的代数运算$\circ$适合结合律，那么对A中任意$n(n\geqslant 3)$个元a_1，a_2，…，a_n来说，用各种加括号的步骤算得的结果都是一样的，但**反之不真。**

例　$A=\{a,\ b,\ c,\ d\}$

	a	b	c	d
a	b	c	d	d
b	d	d	d	d
c	d	d	d	d
d	d	d	d	d

任何四个元之积均为d，即4元结合律成立，但3元结合律不成立：

$$a(aa)=c,\qquad (aa)a=d$$

故　$a(aa)\neq(aa)a$

6. 任何$n(n\geqslant 3)$元结合律均不成立的例

例　$A=\{a,\ b,\ c\}$

	a	b	c
a	b	c	a
b	c	c	c
c	c	c	c

3 元结合律不成立。

$$\begin{cases}(ab)b = cb = c \\ a(bb) = ac = a\end{cases}$$

故 $(ab)b \neq a(ab)$

$n(n>3)$元结合律不成立：

$$\begin{cases}(ab)(b\cdots b) = (ab)c = cc = c \\ a(b(b\cdots b)) = a(bc) = ac = a\end{cases}$$

关于交换律

1. $A=\{$所有实数$\}$，$\circ$是普通减法：$a\circ b = a-b$

这个代数运算不适合交换律：当$a\neq b$时，

$$a-b\neq b-a$$

2. $A=\{a, b, c, d\}$。由表

	a	b	c	d
a	a	b	c	d
b	b	d	a	c
c	c	a	b	d
d	d	c	a	b

所给的代数运算不适合交换律：

$$cd = d, \quad dc = a$$

3. 集合A的代数运算$\circ$适合结合律及交换律，那么计

算 $a_1 \circ a_2 \circ \cdots \circ a_n$时，可以任意掉换元素的次序，但**反之不真。**

例　$A=\{a,\ b,\ c,\ d\}$

代数运算由下表给出：

	a	b	c	d
a	d	c	d	d
b	d	d	d	d
c	d	d	d	d
d	d	d	d	d

任何三元之积均为d，故 3 元结合交换律成立，但 2 元交换律不成立：

$$ab \neq ba$$

4.　$A=\{a,\ b,\ c\}$

	a	b	c
a	b	c	c
b	c	b	b
c	c	b	b

由代数运算表易见 2 元交换律成立。

但 3 元结合律不成立：

$$(ab)c=cc=b,\qquad a(bc)=ab=c$$

又 3 元结合交换律不成立：

$$(ab)c=cc=b,\qquad a(cb)=ab=c$$

5. 3 元结合律成立，2 元交换律不成立，多元结合交换律也不成立。

例如　全体n阶方阵，对矩阵乘法来说，我们已知它

不适合交换律。故

若 $AB \neq BA$，则

$$(EA)B \neq E(BA)$$

6. $A = \{a,\ b\}$

	a	b
a	a	a
b	b	a

3 元结合律成立。

可是由于

$$ab\underbrace{a\cdots a} = aba = a$$
$$ba\underbrace{a\cdots a} = baa = b$$

故n元交换律不成立。

关于分配律

⊕适合结合律。⊙，⊕适合第一(左)分配律，那么 $b\odot(a_1\oplus\cdots\oplus a_n) = (b\odot a_1)\oplus\cdots\oplus(b\odot a_n)$，**但反之不真。**

例 $A = \{a,\ b,\ c\}$

⊕	a	b	c
a	b	c	c
b	c	c	c
c	c	c	c

⊙	a	b	c
a	a	c	c
b	c	c	c
c	c	c	c

易知⊕适合 3 元结合律，并且⊕，⊙适合 3 元分配律：

$$b\odot(a_1\oplus a_2\oplus a_3) = (b\odot a_1)\oplus(b\odot a_2)\oplus(b\odot a_3)$$

但分配律不成立：

$$a\odot(a\oplus a)=a\odot b=c$$
$$(a\odot a)\oplus(a\odot a)=a\oplus a=b$$

§ 3　同态、同构

定义　　一个A到$\overline{A}$的映射ϕ，叫做一个对于代数运算$\circ$和$\overline{\circ}$来说的A到$\overline{A}$的**同态映射**，假如在ϕ之下，不管a和b是A的哪两个元，只要

$$a\to\overline{a},\qquad b\to\overline{b}$$

就有

$$a\circ b\to\overline{a}\,\overline{\circ}\,\overline{b}$$

定义　　假如对于代数运算$\circ$和$\overline{\circ}$来说，有一个A到$\overline{A}$的满射的同态映射存在，我们就说，这个映射是一个**同态满射**，并说，对于代数运算$\circ$和$\overline{\circ}$来说，A与$\overline{A}$**同态**。

定义　　我们说，一个A与$\overline{A}$间的一一映射ϕ是一个对于代数运算$\circ$与$\overline{\circ}$来说的，A与$\overline{A}$间的**同构映射**，假如在ϕ之下，不管a，b是A的哪两个元，只要

$$a\to\overline{a},\qquad b\to\overline{b}$$

就有

$$a\circ b\to\overline{a}\,\overline{\circ}\,\overline{b}$$

这时，我们也说，对于代数运算$\circ$与$\overline{\circ}$来说，A与$\overline{A}$同构。记之以

$$A\simeq\overline{A}$$

定义　　对于$\circ$与$\circ$来说的一个A与A间的同构映射叫做一个对于$\circ$来说的A的**自同构**。

1．　$A=\{$所有整数$\}$，A的代数运算是普通加法；

$\overline{A}=\{1,\ -1\}$，$\overline{A}$的代数运算是普通乘法。

ϕ：　　　$a\rightarrow -1$

是A到$\overline{A}$的映射，但不是同态映射。因为

$$a\rightarrow -1$$
$$b\rightarrow -1$$
$$a+b\rightarrow -1\neq(-1)(-1)$$

2.　$A=\{$所有整数$\}$，A的代数运算是普通加法；

$\overline{A}=\{1,\ -1\}$，$\overline{A}$的代数运算是普通乘法。

ϕ：　$\begin{cases}a\rightarrow 1, & 若a是偶数\\ a\rightarrow -1, & 若a是奇数\end{cases}$

是A到$\overline{A}$的同态满射，但不是A与$\overline{A}$间的同构映射。

3.　$A=\{$所有整数$\}$，A的代数运算是普通加法；

$\overline{A}=\{1,\ -1\}$，$\overline{A}$的代数运算是普通乘法。

ϕ：　$\begin{cases}a\rightarrow -1, & 若a是偶数\\ a\rightarrow 1, & 若a是奇数\end{cases}$

不是A到$\overline{A}$的同态满射。

如　　$2+2=4\longrightarrow -1\neq(-1)(-1)$

这个例题提醒我们，虽然这个ϕ不是A到$\overline{A}$的同态满射，并不妨碍在ψ：　$\begin{cases}a\rightarrow 1, & 若a是偶数\\ a\rightarrow -1, & 若a是奇数\end{cases}$

之下，对A的加法与$\overline{A}$的乘法来说，A与$\overline{A}$同态，这是因为只要存在一个满射的同态映射，就说A与$\overline{A}$同态。

4.　$A=\{$所有整数$\}$，A的代数运算是普通乘法；

$\overline{A}=\{1,\ -1\}$。$\overline{A}$的代数运算是普通乘法。

ψ：　$\begin{cases}a\rightarrow 1, & 若a是偶数\\ a\rightarrow -1, & 若a是奇数\end{cases}$

不是A到$\overline{A}$的同态映射，虽然是满射。

如 $\quad 2 \to 1$

$\quad\quad 3 \to -1$

$$2 \times 3 = 6 \longrightarrow 1 \neq 1(-1)$$

这个例题与上例的提醒告诉我们，虽然ψ尽管相同，是否能充当A与$\overline{A}$的同态满射，不能离开A与$\overline{A}$的代数运算，即同一个ψ对前者A的加法与$\overline{A}$的乘法就构成A与$\overline{A}$同态，对后者A的乘法与$\overline{A}$的乘法来说，这个ψ就不能起这样的作用。

5. $A=\{$所有实数$x\}$，A的代数运算是普通乘法。以下映射是不是A到A的一个子集$\overline{A}$的同态满射？

a) $x \to |x|$ $\quad$ b) $x \to 2x$

c) $x \to x^2$ $\quad$ d) $x \to -x$

我们的回答是：

a) 是A到$\overline{A}=\{$所有$\geqslant 0$的实数$\}$的同态满射，但不是同构映射。

b) 由于$xy \to 2xy \neq (2x)(2y)$ （除非$xy=0$），故$x \to 2x$不是A到A的一个子集$\overline{A}$的同态满射。

c) 易知$x \to x^2$是A到A的一个子集$\overline{A}=\{$所有$\geqslant 0$的实数$\}$的同态满射，但不是同构映射。

d) 一般说来 $\quad -(xy) \neq (-x)(-y)$

所以$x \to -x$不是A到A的一个子集$\overline{A}$的同态满射。

这个例题说明，同态满射，既要是满射又要保持运算。

同构还要要求是一一映射。

6. $\quad A=\{a,\ b,\ c\}$，代数运算由下表给定

	a	b	c
a	c	c	c
b	c	c	c
c	c	c	c

找出所有A的一一变换，对于代数运算来说，这些一一变换是否都是A的自同构？

我们说，所有A的一一变换有以下6个：

τ_1： $a\to a$， $b\to b$， $c\to c$；

τ_2： $a\to b$， $b\to a$， $c\to c$；

τ_3： $a\to b$， $b\to c$， $c\to a$；

τ_4： $a\to c$， $b\to b$， $c\to a$；

τ_5： $a\to c$， $b\to a$， $c\to b$；

τ_6： $a\to a$， $b\to c$， $c\to b$。

容易验证τ_1及τ_2是A的自同构，而τ_3，τ_4，τ_5，τ_6不是A的自同构。

7. 假定对于代数运算$\circ$和$\bar{\circ}$来说，A与$\bar{A}$同态，那么

（i） 若$\circ$适合结合律，$\bar{\circ}$也适合结合律；

（ii） 若$\circ$适合交换律，$\bar{\circ}$也适合交换律，但反之不真。

例1 $A=$\{所有有理数\}，代数运算$\circ$：$a\circ b=-a-b$；

$\bar{A}=\{1\}$，代数运算$\bar{\circ}$是普通乘法。

ϕ： $a\to 1$

显然是A到$\bar{A}$的同态满射。

而$\bar{\circ}$适合结合律也是显然的；但$\circ$不适合结合律：

$$(2\circ 1)\circ 1=(-2-1)\circ 1=3-1=2$$

$$2\circ(1\circ 1)=2\circ(-1-1)=-2-(-2)=0$$

即 $(2\circ1)\circ1\neq2\circ(1\circ1)$

例2 A={所有有理数}，代数运算$\circ$：$a\circ b=b$；

$\overline{A}=\{1\}$，代数运算$\overline{\circ}$是普通乘法。

ϕ： $a\to1$

而$\overline{\circ}$适合交换律，但$\circ$不适合交换律：

$3\circ2=2\neq3=2\circ3$

8. 假定$\odot$，$\oplus$都是集合A的代数运算，$\overline{\odot}$，$\overline{\oplus}$都是集合$\overline{A}$的代算运算，并且存在一个A到$\overline{A}$的满射ϕ，使得A与$\overline{A}$对于代数运算$\odot$，$\overline{\odot}$来说同态，对于代数运算$\oplus$，$\overline{\oplus}$来说也同态，那么

(i) 若$\odot$，$\oplus$适合第一分配律，$\overline{\odot}$，$\overline{\oplus}$也适合第一分配律；

(ii) 若$\odot$，$\oplus$适合第二分配律，$\overline{\odot}$，$\overline{\oplus}$也适合第二分配律。但反之不真。

例 A={所有有理数}，代数运算

$\odot$： $a\odot b=a+b$； $\oplus$： $a\oplus b=a+b$

$\overline{A}=\{0\}$， 代数运算

$\overline{\odot}$： 普通乘法； $\overline{\oplus}$：普通加法。

ϕ： $a\to0$

对两对代数运算来说，A与$\overline{A}$同态。

显然$\overline{\odot}$，$\overline{\oplus}$适合两个分配律。

但$\odot$，$\oplus$不适合两个分配律：

$1\odot(1\oplus1)=3\neq4=(1\odot1)\oplus(1\odot1)$

$(1\oplus1)\odot1=3\neq4=(1\odot1)\oplus(1\odot)$。

9. A={所有有理数}，A的代数运算是普通加法；

$\overline{A}$={所有$\neq0$的有理数}，$\overline{A}$的代数运算是普通乘

法。

可以证明，对于给定的代数运算来说，A与$\overline{A}$间没有同构映射存在。

证　设A与$\overline{A}$间有同构映射ϕ存在，先看在ϕ之下0的象：

$$0 \longrightarrow \overline{a_0}$$

再看在ϕ之下某一元a的象：

$$a \longrightarrow \overline{a}$$

那么　$0+a \longrightarrow \overline{a_0}\,\overline{a}$

但　$0+a=a$

所以　$\overline{a_0}\,\overline{a}=\overline{a}$

$\overline{a} \neq 0$，故必有$\overline{a_0}=1$

即　$0 \longrightarrow 1$

对$-1 \in \overline{A}$来说，在ϕ之下设有$x \in A$，而$x \neq 0$

$$x \longrightarrow -1$$

由于ϕ是同构映射，于是$x+x=2x \longrightarrow 1=(-1)(-1)$，但又知，$0 \longrightarrow 1$，故$2x=0$，从而$x=0$，与$x \neq 0$矛盾。

所以，A与$\overline{A}$间，对给定的代数运算来说，不存在同构映射。

另证　若$A \simeq \overline{A}$

则$\forall a \in A$有

$$\phi(a)=\phi\left(\frac{a}{2}+\frac{a}{2}\right)=\phi\left(\frac{a}{2}\right)\phi\left(\frac{a}{2}\right)>0$$

故ϕ不是满射。

§4　等价关系

A是一个集合，$D=\{$对，错$\}$。

定义　$A\times A$到D的一个映射R叫做A的元间的一个**关系**。

若$R(a,b)=$对，我们说，a与b符合关系R，记作 aRb。

若$R(a,b)=$错，我们说，a与b不符合关系R。

定义　集合 A 的元间的一个关系$\sim$叫做一个**等价关系**。假如$\sim$满足以下规律：

Ⅰ．反射律：$a\sim a$，不管a是A的哪一个元；

Ⅱ．对称律：$a\sim a\Longrightarrow b\sim a$；

Ⅲ．推移律：$a\sim b$，$b\sim c\Longrightarrow a\sim c$。

以下的例题，说明等价关系所要求的三个条件是独立的。

1． 有人说：假如一个关系R适合对称律和推移律，那么它也适合反射律，他的推论方法是：因为R适合对称律，

$$aRb\Longrightarrow bRa$$

因为适合推移律，

$$aRb,\ bRa\Longrightarrow aRa$$

这个推论方法有什么错误？

对这个问题的解释是，这里的aRa的a是受对称律、推移律约束的而不是集合中任意的a。今举例以示上述推论方法是错误的。

$$A=\{a,b,c\},\qquad D=\{\text{对，错}\}$$

R	a	b	c
a	错	错	错
b	错	对	对
c	错	对	对

由表上直接可以看出 R 适合对称律，至于推移律R也是适合的。

$$bRc,\ cRb \Longrightarrow bRb,$$
$$cRb,\ bRc \Longrightarrow cRc;$$

至于

$$bRc,\ cRc \Longrightarrow bRc,$$
$$bRb,\ bRc \Longrightarrow bRc,$$
$$cRb,\ bRb \Longrightarrow cRb,$$
$$cRc,\ cRb \Longrightarrow cRb$$

是显然的。

但 a与a不符合关系，即$R(a,a)=$错，所以R不适合反射律，这正是说明 I 是独立的。

2. $A=\{1,\ 2,\ 4,\ 6,\ 10\}$

aRb 当且只当$4\,|\,a+b$时

R显然适合对称律，以下证明R适合推移律：

$$4\,|\,a+b,\quad 4\,|\,b+c$$

且 $a=4q_1+\gamma_1$， $c=4q_3+\gamma_3$；由于条件$4\,|\,a+b$，$4\,|\,b+c$ 的限制，$a\neq 1$，$c\neq 1$，又由 A 的元素决定了 $\gamma_1\neq 3$，$\gamma_3\neq 3$；当 $\gamma_1=0$ 可得 $\gamma_3=0$，此时有 $a+c=8$；除此只有$\gamma_1=\gamma_3=2$。

这样 a，c 只能分别为 2，6，10，那么

$a+c$ 只能是 4，8，12，16，20

因而　　$4 \mid a+c \Longrightarrow aRc$。　即$R$适合推移律。

但

　　　$4 \nmid 1+1$，即1与1不符合关系。

R不适合反射律。

3.　　$A=\{a,\ b\}$

R	a	b
a	对	错
b	对	对

R适合反射律。

R适合推移律，显然不适合对称律，这说明Ⅰ是独立的。

4．$A=\{$所有实数$\}$，A 的元间关系$\geqslant$是适合反射律及推移律但不适合对称律。

5.　　$A=\{a,\ b,\ c\}$

R	a	b	c
a	对	对	对
b	对	对	错
c	对	错	对

R适合反射律、对称律，但不适合推移律：

　　　bRa，aRc未必有bRc

第六章　　群

§1　　群的定义

1．群的两个定义

群的第一定义　　一个非空集合G对于一个叫做乘法的代数运算来说作成一个群，假如

I．G对于这个乘法来说是闭的；

II．适合结合律；

III．对G的任二元a，b来说，方程

$$ax=b \text{ 和 } ya=b$$

都在G里有解。

群的第二定义　　一个非空集合G对于一个叫做乘法的代数运算来说作成一个群，假如

I．G对于这个乘法来说是闭的；

II．适合结合律；

IV．G里至少存在一个左单位元e使

$$ea=a$$

这里$\forall a\in G$。

V．对于G的任一元a来说，在G里至少存在一个左逆元a^{-1}，使

$$a^{-1}a=e \text{（这里}e\text{是一个固定左单元）}$$

例 $S=\{a, b\}$

而

	a	b
a	a	b
b	a	b

我们说，S对这样规定的乘法不作成群，因为方程

$$yb=a$$

在S中无解。

2． 群的第二定义中第Ⅴ条是否可换为以下条件：

Ⅴ′． 对于G的任何一个元a至少可以找到G的一个左单位元e'以及一个元a^{-1}使

$$a^{-1}a=e'$$

这个条件正好是忽略了e是一个固定左单元的要求。

我们的回答是不能换，仍取前例

例 $S=\{a, b\}$

	a	b
a	a	b
b	a	b

显然 $ba=a$

$ab=b$

又易见a，b都是S的左单位元。不难知道对乘法来说S满足Ⅰ，Ⅱ，Ⅳ，Ⅴ′，而不满足Ⅴ。这是因为对固定的左单位元a（或b）来说，元b（或a）找不到左逆元。

3． 有限群的定义 一个有乘法的有限非空集合G作成一个群，假如满足Ⅰ，Ⅱ以及Ⅲ′。

Ⅱ′ 消去律： $ax=ax'\longrightarrow x=x'$；

$ya=y'a\longrightarrow y=y'$。

这个定义中对集合 G 要求是有限的。否则，纵然符合Ⅰ，Ⅱ，Ⅱ′，G也未必是群。

例 $G=\{$所有不等于零的整数$\}$

对于普通乘法说G适合Ⅰ，Ⅱ，Ⅱ′，可是不适合Ⅲ。

4. 群元的阶

定义 a是群G的一个元，能够使得

$$a^m=e \qquad (e\text{是群}G\text{的单位元})$$

成立的最小的正整数m叫做a的阶。若这样的一个m不存在就说a是无限阶的。

我们知道，一个有限群的每一个元的阶都有限，那么一个群的元的阶都有限，这个群是不是一定为有限群呢？

例 1的任何次（复数）根的全体构成的集合G，对数的乘法来说作成群，这个群的元是无限多，而其每一个元的阶都有限。

事实上，两个n次单位根的乘积仍是一个n次单位根；

n次单位根、m次单位根的乘积，是一个单位根。

$$\varepsilon^n=1, \qquad \eta^m=1$$

即 $$\varepsilon^{mn}=1, \qquad \eta^{mn}=1$$

所以 $(\varepsilon\eta)^{mn}=1$，当$(m, n)=1$时$\varepsilon\eta$是mn次单位根；

当$(m, n)=d$时$\varepsilon\eta$是$\frac{mn}{d}$次单位根。

n次单位根的逆元仍是一个n次单位根。

$$(e^{-1})^n = (e^n)^{-1} = 1$$

这个例子告诉我们，元素都是有限阶的无限群是存在的。

当然，也有这样的结论：元素都是无限阶的无限群是不存在的，这是因为任何一个群都含有一个单位元e，它的阶是1。

除单位元外的所有元的阶都是无限的群是存在的，例如，整数加群。

再如有理数乘群（所有不为零的有理数对普通乘法），单位元1的阶为1，－1的阶为2，其他元的阶都是无限的。

这方面的例题再给出两个。

例1 设Z_n表示以n为模的剩余类环，G是Z_n上一个不定元x的所有多项式作成的加群，则G的元无限多，然而G的每一个元对加法来说，它的阶有限。

例2 特征为p的无限域对于加法来说构成的群中，每个元的阶都有限。

§2 群的同态

1．若群G与集$\overline{G}$对它们的乘法来说同态，则$\overline{G}$也是群。

我们看，若集$\overline{G}$与群G对它们的乘法来说同态，$\overline{G}$是否成群？回答是$\overline{G}$未必成群。

例1 $\overline{G}$ ＝{所有奇数}，普通乘法。

$G=\{e\}$。 乘法是$ee=e$。在

ϕ: $\bar{a} \longrightarrow e$

之下，$\overline{G}$ 与G同态。

但$\overline{G}$对普通乘法不作成群。

例2 $\overline{G}$ = {所有自然数}，普通加法。而$\overline{G}$不成群。

$G = \{1, -1\}$，普通乘法。

而G作成群，在

$$\phi: \begin{cases} a \longrightarrow 1, & \text{当 } a \text{ 是偶数} \\ a \longrightarrow -1, & \text{当 } a \text{ 是奇数} \end{cases}$$

之下，$\overline{G}$ 与G同态。

2. 若群G与群$\overline{G}$同态，则G的单位元e的象是$\overline{G}$的单位元，G的元a的逆元a^{-1}的象是a的象的逆元。

在同样的条件下，即群G与群$\overline{G}$同态，单位元$\bar{e}$的逆象未必只是G的单位元；还有互逆元的逆象未必互逆。

例 G：整数加群

$\overline{G} = \{e, b, c\}$

	e	b	c
e	e	b	c
b	b	c	e
c	c	e	b

令

$$\phi: \begin{cases} x \longrightarrow e, & \text{当} x \equiv 0\ (3) \\ x \longrightarrow b, & \text{当} x \equiv 1\ (3) \\ x \longrightarrow c, & \text{当} x \equiv 2\ (3) \end{cases}$$

易知在ϕ之下$G \sim \overline{G}$。

而 e 的逆象有 3 ，3 不是G的单位元。

又 b、c互逆，其逆象 4 、5 不互逆。

3. 假定在两个群 G 和$\overline{G}$ 的一个同态映射之下。

$$a \longrightarrow \overline{a}$$

a 与 $\overline{a}$ 的阶是不是一定相同？

我们说，不一定。

例1 仍取上例（即第六章 § 2 — 2 之例）

知
$$3 \longrightarrow e$$
$$4 \longrightarrow b$$
$$5 \longrightarrow c$$

3 、4 、5 的阶都是无限的，而 e 的阶为 1 ，b 的阶为 3 ，c 的阶为 3 。

例2 $G=\left\{1,\ \dfrac{-1+\sqrt{3}i}{2},\ \dfrac{-1-\sqrt{3}i}{2}\right\}$

$\overline{G}=\{1\}$

对普通乘法，G 、$\overline{G}$ 都作成群，且$\phi(x)=1$

（这里$\forall x\in G$，$1\in\overline{G}$）

由ϕ可知 $G\sim\overline{G}$

但 $\dfrac{-1+\sqrt{3}i}{2}$，$\dfrac{-1-\sqrt{3}i}{2}$的阶都是 3 ，而 1 的阶是 1 。

4. 群的自同态满射是否一定是自同构？我们的回答是不一定。

例 $R[x]$是实数域上多项式环，因而是加群。令

ϕ： $f(x)\longrightarrow f'(x)$

ϕ是$R[x]$关于加法的一个自同态满射。但不是一一映射。因为可以在R里取a，b而$a\neq b$，但是在ϕ之下有

$$a \longrightarrow a' = 0$$
$$b \longrightarrow b' = 0$$

所以不是自同构。

§3　几个具体群

1. 变换群

定义　一个集合A的若干个一一变换对变换的乘法作成的群叫做A的一个**变换群**。

定理　G是集合A的若干个变换作成的集合，且G含恒等变换ε，当G对变换乘法作成群时，G一定是变换群。

这个结论的取得，特别重要的一点是假设G含恒等变换ε。假使将这一条件忽略，即便G成群，也未必是变换群。

例　$A=\{1,\ 2\}$

τ：　$1\longrightarrow 1$，　$2\longrightarrow 1$

令　$G=\{\tau\}$

显然　$\tau\tau=\tau$

而G作成群，但G不是变换群，这是因为τ不是一一变换。

进一步说，虽然G含恒等变换ε的条件不能略去，但是可以由其他条件代替。下面以定理形式表示。

定理　G是集合A的若干个变换作成的群，且G含一A的满射变换或单射变换，那么G是变换群。

证 i)　含一满射变换τ。

τ：　$a\longrightarrow a^{\tau}$

因为是A的满射变换，则A的元都有a^{τ}形式。

设　ε是G的单位元，就有

$$(a^{\tau})^{\varepsilon}=a^{\tau\varepsilon}=a^{\tau}$$

这正是说G的单位元ε是恒等变换，即G是变换群。

ii)　　含一单射变换λ

ε是单位元

$$(a^{\varepsilon})^{\lambda}=a^{\varepsilon\lambda}=a^{\lambda}$$

由于λ是单射变换，即异元异象，因而象同其逆象亦同。这样就有

$$a^{\varepsilon}=a$$

亦即说明ε是恒等变换，故G是变换群。

总之，由证明过程可得，变换群的单位元就是恒等变换；而恒等变换就是单位元。

我们还要为以下的问题再举一例：

问题　　假定τ是集合A的一个非一一变换，τ会不会有一个左逆元τ^{-1}，使$\tau^{-1}\tau=\varepsilon$？

答：会有的。

例　　$A=\{1,2,3\cdots\}$

$$1\longrightarrow 1$$
$$2\longrightarrow 1$$
$$3\longrightarrow 2$$
$$4\longrightarrow 3$$
$$\cdots\cdots$$

而

τ^{-1}：　　$1\longrightarrow 1$

$$2\longrightarrow 3$$

$$3 \longrightarrow 4$$
$$4 \longrightarrow 5$$
$$\cdots\cdots$$

τ显然是一个非一一变换。

但　　$\tau^{-1}\tau = \varepsilon$

2．　置换群

1）**定义**　一个有限集合的一个一一变换叫做一个**置换**。

一个有限集合的若干置换作成的一个群叫做一个**置换群**。

一个包含n个元的集合的全体置换作成的群叫做n**次对称群**。用S_n表示。

一个n个元的集合的一个置换叫做**k一循环置换**。假如它把a_{i_1}变到a_{i_2}，a_{i_2}变到a_{i_3}，…，a_{i_k}变到a_{i_1}，而使得其余的元（假如还有的话）不变。

2）　一个置换不一定是循环置换。

例　关于4个元集合的置换

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix}$$

就不是一个循环置换。

3）**定理**　每一个n个元的置换都可以写成若干互相没有共同数字（不相连）的循环置换的乘积。

这并不排斥一个n个元的置换可以写成若干有共同数字（相连）的循环置换的乘积

例　一个5个元的置换。

$$(25) = (12)(15)(12)$$

$$= (15)(12)(15)$$

$$= (45)(34)(23)(34)(45)$$

同时给出表示成相连的乘积不是唯一的。

4） $S_3 = \{(1), (12), (13), (23), (123), (132)\}$ 是有限非交换群，而且是元数最少的非交换群。

3. 循环群

定义 若一个群G的每一个元都是G的某一个固定元a的乘方，就把G叫做**循环群**，也说G是由a生成的。以

$$G = (a)$$

表示。a叫做G的一个**生成元**。

1） a^m不一定是（a^m）中a的最小正方幂。

例 6元循环群$G = (a)$

则 $$(a) = (a^5)$$

2） $G \sim \overline{G}$，若G是循环群，则$\overline{G}$也是循环群。

反之不真。

例 $\overline{G} = \{1, -1\} = (-1)$

令 $G = S_3$

ϕ： $\pi \longrightarrow 1$，当π是偶置换；

$\pi \longrightarrow -1$，当π是奇置换。

容易验证

$$G \sim \overline{G}$$

$\overline{G}$是循环群，G是非交换群因而不是循环群，因为循环群一定是交换群。

3）循环群的真子群是循环群，**反之不真**。（有关子群的概念，见下节）

例 G是四元非循环群。

即
$$G=\{e,\ a,\ b,\ c\}$$

	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

G的子群除了平凡子群（e）及G之外，还有$\{e,\ a\}=(a)$，$\{e,\ b\}=(b)$，$\{e,\ c\}=(c)$，且仅有这些，这些真子群都是循环群。

将这个群具体化，可令

$$e=(1)$$
$$a=(12)(34)$$
$$b=(13)(24)$$
$$c=(14)(23)$$

4）　p^n（p素数）元循环群只有$n-1$个（非平凡）真子群，这里循环群的条件是不能省略的。

例　G是非循环四元群，即2^2元群，而不只$2-1=1$个非平凡真子群，实际上有真子群(a)，(b)，(c)。

这个例题同时说明交换群未必是循环群

5）　循环群也可以由多于一个元生成。

例　G是整数加群

$$G=(1),\qquad G=(2,\ 3)$$

§4　子　　群

1.　子群

定义 一个群G的一个子集H叫做G的一个**子群**，若H对于G的乘法来说作成一个群。

1） 子群的定义要求子集H对群G的乘法而言，而不能说，子集H对H的乘法来说成群。

例 $Q=$\{所有有理数\}，Q的乘法是普通加法，则Q对加法来说作成群。

$Q_+=$\{所有正有理数\}，普通乘法。

则Q_+对乘法来说作成群。

虽然Q_+是Q的子集但不是Q的子群。

2） 构成子群的两个条件是独立的。

定理 一个群G的一个非空子集H作成G的一个子群的充要条件是：

(i) $a,\ b\in H\Longrightarrow ab\in H$

(ii) $a\in H\Longrightarrow a^{-1}\in H$

例1 Z是整数加群，$N=$\{所有自然数\}。N适合(i)而不适合(ii)。

例2 Z是整数加群，$Z^*=$\{所有非零整数\}。Z^*适合(ii)而不适合(i)。

3） 有限群不能和它的真子群同构，无限群能否和它的真子群同构？

例 整数加群和其真子群偶数加群同构。

4） 非交换群的真正子群是否都是非交换的？

例 S_3是非交换群。

$H=\{(1),\ (12)\}$是S_3的一个非平凡子群。

但H是交换群。

这个例题同时告诉我们一个非循环群S_3有一个真正子

群$H=\{(1),(12)\}=[(12)]$是循环群。

5） 一个群的两个不同的子集会不会生成相同的子群？

我们说，群的两个不同的子集可能生成相同的子群。

例 S_3是三次对称群

取 $H_1=\{(123)\}$, $H_2=\{(132)\}$

由H_1生成的和由H_2生成的子群都是

$$H=\{(1),(123),(132)\}$$

2．不变子群

子群的陪集

H是群G的一个子群，规定G的元间的一个关系～，

$$a\sim b，当且只当ab^{-1}\in H$$

容易验证～是一个等价关系，这个等价关系所决定的类叫做子群H的**右陪集**。

包含元a的右陪集用Ha来表示。

类似地，可定义子群H的**左陪集**，包含元a的左陪集用aH来表示。

定义 一个群G的一个子群H的右陪集（或左陪集）的个数叫做H在G里的**指数**。

不变子群，一个群G的一个子群N叫做一个**不变（正规）子群**，假如对于G的每一个元a来说，都有

$$Na=aN$$

一个不变子群N的一个左（或右）陪集叫做N的一个陪集。

1） 一个群的子群的左陪集不一定和它的右陪集一致。

例 群S_3的子群$H=\{(1),(12)\}$的左陪集是

$$(1)H=\{(1),\ (12)\}$$
$$(13)H=\{(13),\ (132)\}$$
$$(23)H=\{(23),\ (123)\}$$

而H的右陪集是

$$H(1)=\{(1),\ (12)\}$$
$$H(13)=\{(13),\ (123)\}$$
$$H(23)=\{(23),\ (132)\}$$

由此说明，H的左、右陪集不一致。

2） **拉格朗日（J.Lagrange）定理** 一个有限群G的子群H的阶能整除G的阶。

但**反之不真**。即若G的阶是n，如果$m|n$，那末G不一定有以m为阶的子群。

例 A_4是交代群，A_4的阶为12而$6|12$，但A_4没有以6为阶的子群。

3） 阶是素数的群一定是循环群，**反之不真**。

例 以6为模的剩余类加群是循环群，但其阶是合数6。

4） 陪集$Ha=Hb$，未必有$a=b$。

例 取S_3的一个子群$H=\{(1),\ (123),\ (132)\}$可以知道

$$H(23)=H(13)$$

但(23)与(13)不等。

5） 子集的积

定义 设S_1，S_2，$\cdots$，S_m是一个群G的m个子集，由所有可以写成

$$s_1s_2\cdots s_m \qquad (s_i\in S_i)$$

形式的G的元作成的集合叫做S_1，S_2，…，S_m的**乘积**，这个乘积用

$$S_1S_2\cdots S_m$$

表示。

我们知道：当H是子群时，有$HH=H$，但**反之不真**，也就是说，当$HH=H$时，H不一定成群。

例 $Q^*=\{$所有非零有理数$\}$，对普通乘法作成群。

取Q^*的子集$H=\{$所有奇数$\}$，

则有

$$HH=H$$

但H不是群。

再举一个例题说明：

一个群的两个子群之积未必还是子群。

例 取S_3的两个子群

$H_1=[(12)]$，　$H_2=[(23)]$

则 $H_1H_2=\{(1),(23),(12),(132)\}$ 不作成子群。

6） 子群具有传递性，不变子群是否也具有传递性？意即：N是群G的不变子群，N_1是N的不变子群，N_1是否一定是G的不变子群？

我们说未必。

例 取$G=S_4$

$N=\{(1),(12)(34),(13)(24),(14)(23)\}$

$N_1=\{(1),(14)(23)\}$

易知N是G的子群，N_1是N的子群，并且N是G的不变子群。

因为N是阶为4的群，所以为交换群，故其子群N_1是不变子群。

但是N_1却不是G的不变子群。原因是：

$$(34)^{-1}[(14)(23)](34)=(13)(24)\bar{\in} N_1$$

7） 交换群的任何一个子群都是不变子群．**反之不真，**也就是说，有这样的非交换群存在，它的任何一个子群都是不变子群。

这样的非交换群称为**汉密尔顿群。**

汉密尔顿群之例

取S_8的两个元$\pi_1=(1\ 2\ 3\ 4)(5\ 6\ 7\ 8)$

$\pi_2=(1\ 5\ 3\ 7)(2\ 8\ 4\ 6)$

由π_1、π_2生成子群K.

不难直接验证可得

$$\pi_1^4=\varepsilon \qquad (\varepsilon=(1))$$

$$\pi_2^4=\varepsilon$$

$$\pi_1^2=\pi_2^2$$

$$\pi_1\pi_2\pi_1=\pi_2$$

因而 $K=\{\varepsilon,\ \pi_1,\ \pi_2,\ \pi_1\pi_2,\ \pi_2\pi_1,\ \pi_1^2,\ \pi_1^3,\ \pi_2^3\}$

其中 $\pi_1\pi_2=(1\ 8\ 3\ 6)(2\ 7\ 4\ 5)$

$\pi_2\pi_1=(1\ 6\ 3\ 8)(2\ 5\ 4\ 7)$

$\pi_1^2=\pi_2^2=(13)(24)(57)(68)$

$\pi_1^3=(1\ 4\ 3\ 2)(5\ 8\ 7\ 6)$

$\pi_2^3=(1\ 7\ 3\ 5)(2\ 6\ 4\ 8)$

显然得出K是以8为阶的非交换群。

由拉格朗日定理，群K中非平凡子群的阶必为2或4，

实际上，K中有

唯一一个2阶子群$N_1=(\pi_1^2)$，

三个4阶子群：$N_2=(\pi_1)$，$N_3=(\pi_2)$，$N_4=(\pi_1\pi_2)$。

可以验证，这四个子群都是K的不变子群。

总之，K是非交换群而它的所有子群都是不变子群，亦即K是汉密尔顿群。

8）一个子群H的右陪集集S_r和左陪集集S_l间存在一个一一映射。

这个一一映射是

$$\phi: \qquad Ha \longrightarrow a^{-1}H$$

现在我们问

$$Ha \longrightarrow aH$$

是不是S_r与S_l间的一一映射，我们说未必。

例 $G=S_3$，$H=\{(1),(12)\}$是G的子群。

$H(13)=\{(13),(123)\} \longrightarrow (13)H=\{(13),(132)\}$

$H(123)=\{(123),(13)\} \longrightarrow (123)H=\{(123),(23)\}$

$$H(13)=H(123)$$

但 $$(13)H \neq (123)H$$

所以 $Ha \longrightarrow aH$ 不是S_r到S_l的一个映射。

9） 一个交换群G的每一个子群H都是不变子群。

我们不能说，任一群的交换子群都是不变子群。

例 $G=S_3$，$H=\{(1),(12)\}$是S_3的一个交换子群，但H不是S_3的不变子群。

$$(132)\in S_3 \text{而} (132)^{-1}=(123)$$

$$(132)(12)(123)=(23)\notin H$$

即 H是交换群但不是S_3的不变子群。

§ 5 商　　群

定义　一个群G的一个不变子群N的陪集所作成的群叫做一个**商群**，用G/N表示。

可以证明，“交换群的商群还是交换群”，而**反之不真**。也就是说，有非交换群的商群也是交换群。

在举例之前，先介绍一个概念。

换位子：一个群G的可以写成$a^{-1}b^{-1}ab$形式的元叫做**换位子**。

例　G是一个群。

$C=\{$所有G的有限个换位子的乘积$\}$

首先，C是子群。

我们说，e是换位子。

因为$e=e^{-1}e^{-1}ee$，所以$e\in C$，故C非空。

（有限个换位子的乘积）·（有限个换位子的乘积）

＝有限个换位子的乘积。故C对G的乘法是闭的。

由于$(a^{-1}b^{-1}ab)^{-1}=b^{-1}a^{-1}ba$是换位子，故（有限个换位子的乘积）的逆仍为（有限个换位子的乘积）。即若$c\in C$，则$c^{-1}\in C$。

这样C是子群，进一步证明C是不变子群。

$c\in C$，　　$g\in G$

由$gcg^{-1}c^{-1}\in C$，有$(gcg^{-1}c^{-1})c\in C$

此即　$gcg^{-1}\in C$，所以C是不变子群。

现在可以证明G/C是交换群。

x、$y\in G$，则$x^{-1}y^{-1}xy\in C$

即　　$x^{-1}y^{-1}xy=c$　就有$xy=yxc$

故　　$xy\in yxC$，因而

$$xyC=yxC$$

即　　$(xC)(yC)=(yC)(xC)$

所以G/C是交换群。

另一个问题是关于集合的象及逆象。

先定义这两个概念。

令ϕ是集合A到集合$\overline{A}$的一个满射。

我们说，$\overline{S}$是A的一个子集S在ϕ之下的**象**，假如$\overline{S}$刚好包含所有S的元在ϕ之下的象。

我们说，S是$\overline{A}$的一个子集$\overline{S}$在ϕ之下的**逆象**，假如S刚好包含所有$\overline{S}$的元在ϕ之下的逆象。

我们的结论是：若S是$\overline{S}$的逆象，$\overline{S}$一定是S的象。

反之不真，就是说，若$\overline{S}$是S的象，S不一定是$\overline{S}$的逆象。

例　设$A=\{1, 2, 3, 4, 5, 6\}$，$\overline{A}=\{1, 2\}$

$$\phi:\quad 1\longrightarrow 1,\quad 4\longrightarrow 2$$
$$2\longrightarrow 2,\quad 5\longrightarrow 1$$
$$3\longrightarrow 1,\quad 6\longrightarrow 2$$

令　$S=\{1, 3\}$

在ϕ之下

$$\overline{S}=\{1\}$$

但$\overline{S}$的逆象是$\{1, 3, 5\}$

再一个问题是：一个群G同它的商群G/N同态。

当$G\sim G/N$是指自然同态时，那么这个核就是N。

当$G\sim G/N$的同态映射不是自然同态，那么这个核就未必是N。

例　$G=\{e, a, b, c\}$

	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

是非循环四元群。

$N=\{e, a\}$ 是G的不变子群。

这时$G/N=\{Ne, Nb\}$

令ϕ:　$x \longrightarrow Nx$　$(x \in G)$

使得　$G \sim G/N$

ϕ的同态核就是N。

令ψ:　$e \longrightarrow Ne$

$b \longrightarrow Ne$

$c \longrightarrow Nb$

$a \longrightarrow Nb$

容易验证ψ使得$G \sim G/N$，但ψ不是自然同态。

ψ的同态核是$N_1=\{e, b\}$，显然$N_1 \neq N$，根据定理易知

$$G/N_1 \cong G/N$$

这同时说明，对G来说，两个商群同构，两个不变子群N_1与N未必一致。

第七章　环 与 域

§1　环、域

先给出环的定义。

定义　一个集合R叫做一个环，假如

i）R是一个加群，换一句话说，R对于一个叫做加法的代数运算来说作成一个交换群；

ii）R对于另一个叫做乘法的代数运算来说是闭的；

iii）这个乘法适合结合律：

$$a(bc)=(ab)c$$

不管a，b，c是R的哪三个元；

iv）两个分配律都成立：

$$a(b+c)=ab+ac$$

$$(b+c)a=ba+ca$$

不管a，b，c是R的哪三个元。

1．环

1）关于交换律

以下给出乘法不适合交换律的环的例，即所谓非交换环的例。

例 1　$R_{n\times n}=\left\{\begin{pmatrix}a_{11}\cdots a_{1n}\\ \vdots \quad \vdots\\ a_{n1}\cdots a_{nn}\end{pmatrix}\middle| a_{ij}\in R\right\}$，对矩阵加法与

矩阵乘法，容易验证作成一个环，是非交换环。

例 2　$R=\{0, a, b, c\}$，加法和乘法分别由以下两个表给定：

+	0	a	b	c
0	0	a	b	c
a	a	0	c	b
b	b	c	0	a
c	c	b	a	0

·	0	a	b	c
0	0	0	0	0
a	0	0	0	0
b	0	a	b	c
c	0	a	b	c

能够验证R作成一个环。

因为　$ab=0$，$ba=a$

所以　　　$ab\neq ba$

即　R是非交换环。

2）关于单位元

以下给出无单位元的环，其中包含有左单位元而无右单位元或有右单位元而无左单位元的情形。

例 1　偶数环没有单位元。

例 2　有两个左单位元而无右单位元的例。

$R=\{0, a, b, c\}$，以下是加法、乘法表

+	0	a	b	c
0	0	a	b	c
a	a	0	c	b
b	b	c	0	a
c	c	b	a	0

·	0	a	b	c
0	0	0	0	0
a	0	0	0	0
b	0	a	b	c
c	0	a	b	c

R作成环。

由乘法表直接看出b、c都是R的左单位元而没有右单位

元。

例 3　有无限多个左单位元而无右单位元的例。

$R=\{(a,\ b)|\ a,\ b\in Z\}$　　　（Z 是整数集）

对于加法　$(a,\ b)+(c,\ d)=(a+c,\ b+d)$以及乘法

$(a,\ b)(c,\ d)=(ac,\ ad)$来说，R作成环。

$$(1,\ b)(c,\ d)=(c,\ d)$$

所以（1，b）是左单位元，由于b是任意整数，因而有无限多左单位元。

我们说，没有右单位元。

如果　$(c,\ d)(x,\ y)=(c,\ d)$

即　　$(cx,\ cy)=(c,\ d)$

则应有　$cx=c$，因而$x=1$，

$$cy=d,\ \text{因而}\ y=\frac{d}{c},\ \text{此时}\frac{d}{c}\text{未必是整数。}$$

关于有多个右单位元而无左单位元的例题可以类似地举出，这里就从略了。

例 4　我们知道“对于有单位元的环来说，加法适合交换律是环定义里其它条件的结果。”

但**反之不真**，即加法适合交换律的环未必有单位元。如偶数环。

3）关于零因子

定义　在一个环里若

$$a\neq 0,\ b\neq 0\quad\text{而}\quad ab=0$$

就说a是这个环的一个**左零因子**，b是一个**右零因子**。

例 1　模 6 的剩余类环Z_6有零因子。

$$[2]\neq[0],\ [3]\neq[0]$$

而
$$[2][3]=[6]=[0]$$

例 2 n阶矩阵环$R_{n\times n}$有零因子。

$$\begin{pmatrix}1&&&\\&0&&\\&&0&\\&&&\ddots&\\&&&&0\end{pmatrix}\begin{pmatrix}0&&&\\&1&&\\&&0&\\&&&\ddots&\\&&&&0\end{pmatrix}=\begin{pmatrix}0&&&\\&0&&\\&&0&\\&&&\ddots&\\&&&&0\end{pmatrix}$$

例 3 $R=\{0, a, b, c\}$

+	0	a	b	c
0	0	a	b	c
a	a	0	c	b
b	b	c	0	a
c	c	b	a	0

·	0	a	b	c
0	0	0	0	0
a	0	0	0	0
b	0	a	b	c
c	0	a	b	c

$$aa=0$$

故a既是左零因子又是右零因子。

$$ab=0, \quad ac=0$$

则b、c是右零因子，易知其不是左零因子。

例 4 单位元显然不是零因子，但左（右）单位元就未必不是零因子。

$$R=\left\{\begin{pmatrix}a&b\\0&0\end{pmatrix}\middle| a, b\in Z\right\}$$

R对于矩阵加法和矩阵乘法作成环。

$$\begin{pmatrix}1&c\\0&0\end{pmatrix}\text{是左单位元}$$

但
$$\begin{pmatrix}0&d\\0&0\end{pmatrix}\begin{pmatrix}1&c\\0&0\end{pmatrix}=\begin{pmatrix}0&0\\0&0\end{pmatrix}$$

这就是说，左单位元$\begin{pmatrix} 1 & c \\ 0 & 0 \end{pmatrix}$是右零因子。

例 5　一个有零因子的环里，消去律不成立，举一例以验证之。

$$Z_{2\times 2}=\left\{\begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix} \middle| a_{ij}\in Z\right\}$$

取 $$\begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix}\neq\begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$$

$$\begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix}\begin{pmatrix} b & 0 \\ c & d \end{pmatrix}=\begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix}\begin{pmatrix} b & 0 \\ h & k \end{pmatrix}$$

其中　$c\neq h$。

而 $$\begin{pmatrix} b & 0 \\ c & d \end{pmatrix}\neq\begin{pmatrix} b & 0 \\ h & k \end{pmatrix}$$

同样，另一个消去律也不成立。

4）关于逆元

定义　有单位元环的一个元b叫做元a的一个**左（右）逆元**。假如

$$ba=1\quad(ab=1)$$

有单位元的环的一个元b叫做元a的一个**逆元**。假如

$$ba=ab=1$$

例 1　整数环中除±1而外的元是既无左逆元又无右逆元。

例 2　$R=\{$每行每列只有有限多数$\neq 0$的无限整数矩阵$\}$

R是有单位元的环。

$$E=\begin{pmatrix}1&&\\&1&\\&&\ddots\end{pmatrix}$$

是（两侧）单位元

令

$$A=\begin{pmatrix}0&1&0&0&0&\cdots\\0&0&1&0&0&\cdots\\0&0&0&1&0&\cdots\\&&&&\ddots&\end{pmatrix}$$

$$C_n=\begin{pmatrix}\overbrace{1\quad 1\quad 1\quad \cdots\quad 1}^{n\text{个}}&0&\cdots\\1\quad 0\quad 0\quad \cdots\quad 0&0&\cdots\\0\quad 1\quad 0\quad \cdots\quad 0&0&\cdots\\ \ddots&&\end{pmatrix}$$

则

$$AC_n=E=\begin{pmatrix}1&&\\&1&\\&&\ddots\end{pmatrix}\qquad n=0,\ 1,\ 2\cdots$$

这就是说A有多个右逆元而无左逆元。

类似地可以举出有多个左逆元而无右逆元的例。

2．域

整环的定义 一个环R叫做一个**整环**，若

i）乘法适合交换律：

$$ab=ba$$

ii）R有单位元 1：

$$1a=a1=a$$

iii）R没有零因子：

$$ab=0 \Rightarrow a=0 \text{ 或 } b=0.$$

这里a、b是R的任意元。

除环的定义 一个环R叫做**除环**，若

i）R至少包含一个不等于零的元；

ii）R有一个单位元；

iii）R的每一个不等于零的元有一个逆元。

域的定义 一个交换除环叫做一个**域**。

1）域之等价定义

集合F对于它的加法与乘法作成一个域，假如满足以下八个条件：

i）加法交换律：

$a+b=b+a$

ii）加法结合律：

$a+(b+c)=(a+b)+c$

iii）方程可解：

$a+x=b$

iv）乘法交换律：

$ab=ba$

v）乘法结合律：

$a(bc)=(ab)c$

vi）方程有解：

$ax=b \quad (a\neq 0)$

vii）F至少有一个非零元

viii）分配律：

$a(b+c)=ab+ac$

以上a，b，c是F的任意元。

2）构成域的八个条件是独立的。

我们说，某一个条件是独立的，就要举一个例，这个例满足其他七个条件，只是不满足某一个条件，应该注意的是这与验证不作成域是有区别的，不作成域，只要有一条不被满足就行了，不去管其他七条的情形。

例 1　条件i）是独立的。

$F_1=\{$所有正有理数$\}$

加法：$a\oplus b=b$

乘法：$a\odot b=ab$

首先，不适合加法交换律：

$$2\oplus3=3,\quad 3\oplus2=2$$

容易验证满足其他七个条件。

例 2　条件ii）是独立的。

$F_2=\{$所有有理数$\}$

加法：$a\oplus b=-a-b$

乘法：$a\odot b=ab$

首先，不适合加法结合律：

$$\begin{aligned}2\oplus(3\oplus4)&=2\oplus(-3-4)=2\oplus(-7)\\&=-2-(-7)=5\\(2\oplus3)\oplus4&=(-2-3)\oplus4=(-5)\oplus4\\&=-(-5)-4=1\end{aligned}$$

容易验证满足其他七个条件。

例 3　条件iii）是独立的。

$F_3=\{$所有正有理数$\}$

加法：$a\oplus b=a+b$

乘法：$a \odot b = ab$

首先，方程

$$3 + x = 2$$

在F_3中无解。

容易验证满足其他七个条件。

例 4　条件iv）是独立的。

$F_4 = \{$所有有理数$\}$

加法：$a \oplus b = a + b$

乘法：$a \odot b = b$

首先，不适合乘法交换律：

$$2 \odot 3 = 3, \quad 3 \odot 2 = 2$$

容易验证满足其他七个条件。

例 5　条件v）是独立的。

$F_5 = \{(a_1, a_2) | a_1, a_2$任意实数$\}$

加法：$(a_1, a_2) \oplus (b_1, b_2) = (a_1 + b_1, a_2 + b_2)$

乘法：$(a_1, a_2) \odot (b_1, b_2)$

$$= (a_1 b_1 - a_2 b_2, -a_1 b_2 - a_2 b_1)$$

首先，不适合乘法结合律：

$$(1, 2) \odot [(3, 4) \odot (5, 6)] = (1, 2) \odot (-9, -38)$$
$$= (67, 56)$$
$$[(1, 2) \odot (3, 4)] \odot (5, 6) = (-5, -10) \odot (5, 6)$$
$$= (35, 80)$$

容易验证满足其他七个条件。

例 6　条件vi）是独立的。

$F_6 = \{$所有整数$\}$

加法：$a \oplus b = a + b$

乘法：$a \odot b = ab$

首先，方程

$$2x = 3$$

在F_6中没有解。

容易验证满足其他七个条件。

例 7 条件vii）是独立的。

$F_7 = \{0\}$

加法：$a \oplus b = a + b$

乘法：$a \odot b = ab$

首先，不满足F_7至少含有一个非零元。

容易验证满足其他七个条件。

例 8 条件viii）是独立的。

$F_8 = \{$所有有理数$\}$

加法：$a \oplus b = a + b$

乘法：$a \odot b = a + b$

首先，不适合分配律：

$$2 \odot (1 \oplus 1) = 2 \odot 2 = 4$$

$$(2 \odot 1) \oplus (2 \odot 1) = 3 \oplus 3 = 6$$

容易验证满足其他七个条件。

以上八个例题也是八个作不成域的例。

3）域一定是除环，除环未必是域。

例 $R = \{$所有复数对$(\alpha, \beta)\}$

加法：$(\alpha_1, \beta_1) + (\alpha_2, \beta_2) = (\alpha_1 + \alpha_2, \beta_1 + \beta_2)$

乘法：$(\alpha_1, \beta_1)(\alpha_2, \beta_2) = (\alpha_1\alpha_2 - \beta_1\overline{\beta_2}, \alpha_1\beta_2 + \beta_1\overline{\alpha_2})$

容易验证R是一个除环。

但R不是交换环

$$(i, 0)(0, 1) = (0, i)$$
$$(0, 1)(i, 0) = (0, -i)$$

因而R不是域。

4）在域上的两个多项式相等一定得到此二多项式函数相等，**反之不真**。即两个多项式函数相等，此二多项式未必相等。

例 见多项式一章中所举之例。

3. 特征

定义 一个无零因子环R的非零元的相同的（对加法来说的）阶叫做环R的**特征**。

1）特征的定义限制环是无零因子。若没有此限制情形就不同了，也就是说，在一个环里，可能某一个不等于零的元对加法来说的阶是无限，另一个不等于零的元的阶却是有限的。

例 1 $R = \{(hb, kc) \mid \forall hb \in G_1, kc \in G_2\}$

这里加群$G_1 = (b)$，b的阶无限，加群$G_2 = (c)$，c的阶是n。

加法：$(h_1b, k_1c) + (h_2b, k_2c) = (h_1b + h_2b, k_1c + k_2c)$

乘法：$(h_1b, k_1c)(h_2b, k_2c) = (0, 0)$

则R作成环，这个环的元

$(b, 0)$对于加法来说的阶是无限大，

$(0, c)$对于加法来说的阶是n。

例 2 Z_6是以6为模的剩余类环。

$[2]$的阶为3，$[3]$的阶为2。

2）在特征是p的交换环里有

$$(a+b)^p = a^p + b^p$$

推而广之有

$$(a_1+a_2+\cdots+a_m)^p=a_1{}^p+a_2{}^p+\cdots+a_m{}^p$$

以及

$$(a\pm b)^{p^n}=a^{p^n}\pm b^{p^n} \qquad (n\text{是非负整数})$$

3）在域的条件中将乘法对加法的分配律

$$a(b+c)=ab+ac$$

换为加法对乘法的分配律

$$a+(bc)=(a+b)(a+c)$$

是不是仍作成域？

我们的回答是否定的。

因为若能作成域，则将导出矛盾。

域内有单位元1，则有 $1+(1\cdot 1)=(1+1)(1+1)$

为了看起来明显，这里用e代替1，这样就有

$$e+(e\cdot e)=(e+e)(e+e)$$

即 $$2e=2e\cdot 2e$$

若特征$\neq 2$，则$2e\neq 0$，可得$2e=e$因而$e=0$，故矛盾；

若特征$=2$，此时对元e，e，0而言，

$$e+(e\cdot 0)=(e+e)(e+0)$$

$$e=2e$$

$$e=0 \quad \text{亦矛盾。}$$

4．数环、数域

这里给出关于数环、数域几个正面的例题。

1）找出含7与18的最小数环。

含7与18的数环R，则还必须包含

$$18-7=11$$

同样，$11-7=4\in R$，$7-4=3\in R$，$4-3=1\in R$

我们知道，只要$1\in R$，则R包含所有整数，而所有整数确实

作成数环，那么可以说，最小的含 7 与 18 的 数 环就是整数环。关于最小这一点由找法可见。

2）找出含$\sqrt{3}$的最小数环。

欲含$\sqrt{3}$的数环，则需含$n\sqrt{3}$（n为整数）以及（$\sqrt{3}$）^{k}（k 为正整数），归纳起来应含

$$3m+n\sqrt{3} \qquad (m,\ n\text{为整数})$$

形式的数，令

$$R=\{3m+n\sqrt{3} \mid m,\ n\text{为整数}\}$$

容易验证R是含$\sqrt{3}$的数环，至于R是含$\sqrt{3}$的最小数环由找法可见。

3）在整数环Z中找出含 3 而不含 5 的最大数环。

含 3 而不含 5 的数环要包含$3m$（m为整数）形式的数。

而 $R=\{3m \mid m\in Z\}$

确实作成数环。

现在再证明R是Z中含 3 而不含 5 的最大数环。

若R再含一个不是$3m$形式的整数n，那么就有$(n,3)=1$，因而存在整数l、k使得

$$ln+3k=1$$

由于n是R的元，ln 就是R的元以及 $3k$ 是 R 的元，故有 1 是R的元，因此R含所有的整数，故含有 5，所以$\{3m \mid m\in Z\}$是含 3 而不含 5 的Z中的最大数环。

4）$F=R[\sqrt[3]{2}]=\{a+b\sqrt[3]{2}+c\sqrt[3]{4} \mid a,\ b,\ c$ 为任意有理数$\}$

则F是数域。

证 F含有非零元，如$2\in F$。

i）$(a_1+b_1\sqrt[3]{2}+c_1\sqrt[3]{4})\pm(a_2+b_2\sqrt[3]{2}+c_2\sqrt[3]{4})$

$$=(a_1\pm a_2)+(b_1\pm b_2)\sqrt[3]{2}+(c_1\pm c_2)\sqrt[3]{4}\in F$$

ii) $(a_1+b_1\sqrt[3]{2}+c_1\sqrt[3]{4})(a_2+b_2\sqrt[3]{2}+c_2\sqrt[3]{4})$

$$=(a_1a_2+2b_1c_2+2c_1b_2)+(a_1b_2+a_2b_1+2c_1c_2)\times$$
$$\times\sqrt[3]{2}+(a_1c_2+a_2c_1+b_1b_2)\sqrt[3]{4}\in F$$

iii) $\dfrac{a_1+b_1\sqrt[3]{2}+c_1\sqrt[3]{4}}{a_2+b_2\sqrt[3]{2}+c_2\sqrt[3]{4}}$ 这里$a_2+b_2\sqrt[3]{2}+c_2\sqrt[3]{4}$

$\neq 0$

$$=\frac{a_1+b_1\sqrt[3]{2}+c_1\sqrt[3]{4}}{a_2+b_2\sqrt[3]{2}+c_2\sqrt[3]{4}}\times$$

$$\times\frac{(a_2^2-2b_2c_2)+(2c_2^2-a_2b_2)\sqrt[3]{2}+(b_2^2-a_2c_2)\sqrt[3]{4}}{(a_2^2-2b_2c_2)+(2c_2^2-a_2b_2)\sqrt[3]{2}+(b_2^2-a_2c_2)\sqrt[3]{4}}$$

$$=\frac{a_1a_2^2-2a_1b_2c_2+4c_1c_2^2-2a_2b_2c_1+2b_1b_2^2-2a_2b_1c_2}{a_2^3+2b_2^3+4c_2^3-6a_2b_2c_2}$$

$$+\frac{2a_1c_2^2-a_1a_2b_2+a_2^2b_1-2b_1b_2c_2+2b_2^2c_1-2a_2c_1c_2}{a_2^3+2b_2^3+4c_2^3-6a_2b_2c_2}\sqrt[3]{2}$$

$$+\frac{a_1b_2^2-a_1a_2c_2+a_2^2c_1-2b_2c_1c_2+2b_1c_2^2-a_2b_1b_2}{a_2^3+2b_2^3+4c_2^3-6a_2b_2c_2}\times$$

$$\times\sqrt[3]{4}\in F$$

这里 $(a_2^2-2b_2c_2)(2c_2^2-a_2b_2)\sqrt[3]{2}+(b_2^2-a_2c_2)\sqrt[3]{4}\neq 0$

不然 $a_2^2-2b_2c_2=0$ （1）

$2c_2^2-a_2b_2=0$ （2）

$b_2^2-a_2c_2=0$ （3）

因为a_2，b_2，c_2不同时为0，不妨设$a_2\neq 0$（若$a_2=0$，

可设b_2或c_2之一不为0，情况和$a_2 \neq 0$类似地推导），由（3）得c_2并将c_2代入（1）而后得

$$a_2^3 - 2b_2^3 = 0$$

若 $b_2 = 0$，则 $a_2 = 0$，所以$b_2 \neq 0$。

由此得

$$\left(\frac{a_2}{b_2}\right)^3 = 2$$

即

$$\frac{a_2}{b_2} = \sqrt[3]{2} \qquad \text{故矛盾。}$$

§2 子 环

定义 一个环R的一个子集S叫做R的一个**子环**，假如S本身对于R的代数运算来说作成一个环。

以下将分别讨论环与子环关于交换性、零因子、单位元的情形。

1．关于交换性

1）环R是交换环，子环S也是交换环。

例 R是实数环，S＝整数环Z。

2）环R是非交换环，子环S是交换环。

例1 $R = R_{n\times n} = \left\{\begin{pmatrix} a_{11} \cdots a_{1n} \\ \vdots \quad\quad \vdots \\ a_{n1} \cdots a_{nn}\end{pmatrix} \middle| a_{ij}\text{是实数}\right\}$

那么，$R_{n\times n}$是非交换环。

$$S = \left\{\begin{pmatrix} a & & & \\ & 0 & & \\ & & \ddots & \\ & & & 0 \end{pmatrix}_{n\times n} \middle| a\text{是实数}\right\},$$

是$R_{n\times n}$的交换子环。

例 2　$R=\overline{Q}$而$\overline{Q}$是四元数非交换环。

$S=$复数环C，而且是$\overline{Q}$的交换子环。

我们说明一下四元数环$\overline{Q}$。

$\overline{Q}=\{a+bi+cj+dk|\ a,\ b,\ c,\ d$均为实数$\}$

$$i^2=j^2=k^2=-1$$

$$ij=-ji=k,\quad jk=-kj=i,\quad ki=-ik=j$$

加法为　$(a+bi+cj+dk)+(a'+b'i+c'j+d'k)$

$$=(a+a')+(b+b')i+(c+c')j+(d+d')k$$

容易验证$\overline{Q}$是非交换环，其元素称为四元数。

3）环R是非交换环，子环S也是非交换环。

例　$R=R_{3\times 3}=\left\{\begin{pmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{pmatrix}\middle| a_{ij}\text{是实数}\right\}$

$$S=\left\{\begin{pmatrix} 0 & a & b \\ 0 & 0 & c \\ 0 & 0 & 0 \end{pmatrix}\middle| a,\ b,\ c\text{是实数}\right\}$$

易知S是$R_{3\times 3}$的子环，而且是非交换的：

$$\begin{pmatrix} 0 & 1 & 2 \\ 0 & 0 & 3 \\ 0 & 0 & 0 \end{pmatrix}\begin{pmatrix} 0 & 4 & 5 \\ 0 & 0 & 6 \\ 0 & 0 & 0 \end{pmatrix}=\begin{pmatrix} 0 & 0 & 6 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}$$

$$\begin{pmatrix} 0 & 4 & 5 \\ 0 & 0 & 6 \\ 0 & 0 & 0 \end{pmatrix}\begin{pmatrix} 0 & 1 & 2 \\ 0 & 0 & 3 \\ 0 & 0 & 0 \end{pmatrix}=\begin{pmatrix} 0 & 0 & 12 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}$$

2．关于零因子

1）环R无零因子，子环S也无零因子。

例 $R=$整数环Z，S是偶数环。

2）环R有零因子，子环S有零因子。

例 $R=R_{2\times2}=\left\{\begin{pmatrix}a_{11} & a_{12}\\ a_{21} & a_{22}\end{pmatrix}\middle| a_{ij}\text{是实数}\right\}$

$R_{2\times2}$有零因子。

$$S=\left\{\begin{pmatrix}a_1 & \\ & a_2\end{pmatrix}\middle| a_1,\ a_2\text{是实数}\right\}$$

易知S是$R_{2\times2}$的子环且有零因子：

$$\begin{pmatrix}1 & \\ & 0\end{pmatrix}\begin{pmatrix}0 & \\ & 1\end{pmatrix}=\begin{pmatrix}0 & \\ & 0\end{pmatrix}$$

3）环R有零因子，子环S无零因子。

例 $R=R_{2\times2}=\left\{\begin{pmatrix}a_{11} & a_{12}\\ a_{21} & a_{22}\end{pmatrix}\middle| a_{ij}\ \text{是实数}\right\}$

有零因子。

$$S=\left\{\begin{pmatrix}a & \\ & 0\end{pmatrix}\middle| a\text{是实数}\right\}$$

易见，S是$R_{2\times2}$的子环，而S无零因子。

3. 关于单位元

1）环R有单位元，子环 S 也有单位元，而且单位元一致。

例 $R=$有理数环Q，单位元为1。

子环$S=$整数环Z，单位元为1，故单位元一致。

2）环R有单位元，子环 S 也有单位元，但单位元不一致。

例 $R=R_{2\times2}=\left\{\begin{pmatrix}a_{11} & a_{12}\\ a_{21} & a_{22}\end{pmatrix}\middle| a_{ij}\text{是实数}\right\}$

有单位元$\begin{pmatrix}1 & \\ & 1\end{pmatrix}$。

$$S=\left\{\begin{pmatrix}a & \\ & 0\end{pmatrix}\middle| a\text{是实数}\right\}$$

易知S是$R_{2\times2}$的子环，而S的单位元是$\begin{pmatrix}1 & \\ & 0\end{pmatrix}$，但单位元不一致。

3）环R有单位元，子环S无单位元。

例 R是整数环Z，有单位元1，而子环S是偶数环，没有单位元。

4）环R无单位元，子环S有位单元。

例 $R=\left\{\begin{pmatrix}a & 0\\ 0 & b\end{pmatrix}\middle| a,\ b\text{是整数}\right\}$

加法：$\begin{pmatrix}a & 0\\ 0 & b\end{pmatrix}+\begin{pmatrix}c & 0\\ 0 & d\end{pmatrix}=\begin{pmatrix}a+c & 0\\ 0 & b+d\end{pmatrix}$

乘法：$\begin{pmatrix}a & 0\\ 0 & b\end{pmatrix}\begin{pmatrix}c & 0\\ 0 & d\end{pmatrix}=\begin{pmatrix}ac & 0\\ 0 & 0\end{pmatrix}$

容易验证R是环，R显然没有单位元。

而 $S=\left\{\begin{pmatrix}a & 0\\ 0 & 0\end{pmatrix}\middle| a\text{是整数}\right\}$

是R的子环，子环S有单位元$\begin{pmatrix}1 & 0\\ 0 & 0\end{pmatrix}$。

5）环R无单位元，子环S无单位元。

例 R是偶数环，无单位元。

$$S=\{4m \mid m\text{是整数}\}$$

是R的子环，S也没有单位元。

4．关于左、右单位元

这里讨论关于一个环的左、右单位元存在情况。

1）无左单位元也无右单位元。

例 偶数环。

2）有左单位元也有右单位元则一定有唯一左单位元、唯一右单位元且二者相等。

3）有唯一左单位元则此唯一左单位元必为右单位元。

4）有唯一右单位元则此唯一右单位元必为左单位元。

5）有多个（＞1）左单位元而无右单位元。

例1 $R=\left\{\begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix} \middle| a,\ b\text{是整数}\right\}$

易知R对矩阵的加法与矩阵的乘法作成环。

由于 $\begin{pmatrix} 1 & c \\ 0 & 0 \end{pmatrix}\begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix}=\begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix}$

故知

$\begin{pmatrix} 1 & c \\ 0 & 0 \end{pmatrix}$是$R$的左单位元。又由于$c$的任意性，所以有无穷多个左单位元。

因为

$$\begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix}\begin{pmatrix} h & k \\ 0 & 0 \end{pmatrix}=\begin{pmatrix} ah & ak \\ 0 & 0 \end{pmatrix}$$

若令

$$\begin{pmatrix} ah & ak \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix}$$

则有　　$ah = a$　　因而$h = 1$

　　　　$ak = b$　　因而　$k = \frac{b}{a}$

k未必是整数，而且k是由a、b的不同而不同，故R没有右单位元。

例 2　$R = \{(a,\ b) | a,\ b\text{是整数}\}$

规定加法为　$(a,b) + (c,d) = (a+c, b+d)$，

　　乘法为　$(a,b)(c,d) = (ac, ad)$

R为环，有无穷多个左单位元而无右单位元。

§3　环 的 同 态

1．与环同态者未必是环。

定理　若存在一个环R到非空集合$\overline{R}$的满射，使得R与$\overline{R}$对于一对加法以及一对乘法来说都同态，那么$\overline{R}$也是一个环。

反之不真，即存在一个非空集合R到一个环$\overline{R}$的满射，使得R与$\overline{R}$对于一对加法以及一对乘法来说都同态，R未必是一个环。

例　$R = \{\text{所有整数}\}$

加法：$a \oplus b = b$

乘法：$a \odot b = ab$

　　$\overline{R} = \{0\}$是环

ϕ：　　　　$a \longrightarrow 0$

ϕ是R到$\overline{R}$的满射，且R与$\overline{R}$同态。

但R不是环。

2．同态环未必保持反向的交换性。

定理 假定R和$\overline{R}$是两个环，且R与$\overline{R}$同态，若R是交换环，则$\overline{R}$也是交换环；若R有单位元，则$\overline{R}$也有单位元。

反之不真，即在环R与环$\overline{R}$同态条件之下，$\overline{R}$是交换环，R未必是交换环；$\overline{R}$有单位元，R未必有单位元。

例1 $R=R_{n\times n}=\left\{\begin{pmatrix} a_{11} & \cdots & a_{1n} \\ \vdots & & \vdots \\ a_{n1} & \cdots & a_{nn} \end{pmatrix} \middle| a_{ij}\text{是实数}\right\}$，$\overline{R}$是零环，

在两者之间，容易建立满射，且$R_{n\times n}$与$\overline{R}$同态。

$\overline{R}$是交换环，而$R_{n\times n}$是非交换环。

例2 R是偶数环，$\overline{R}$是零环，在两者之间，容易建立R到$\overline{R}$的满射，且R与$\overline{R}$同态。

$\overline{R}$有单位元，但R没有单位元。

例3 $R=\left\{\begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix} \middle| a,\ b\text{是整数}\right\}$

R是没有单位元的非交换环。

$\overline{R}$是整数环Z且为有单位元的交换环。

但在

$$\phi:\quad \begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix} \longrightarrow a$$

之下，R与$\overline{R}(=Z)$同态。

3．关于零因子

例1 环R到环$\overline{R}$有一个同态满射，R没有零因子，$\overline{R}$可以有零因子。

R是整数环Z，$\overline{R}$是以n为模的剩余类环Z_n。

ϕ： $a \longrightarrow [a]$

是Z到Z_n的一个同态满射。

Z没有零因子，而Z_n当n是合数时有零因子。

例 2 环R到环$\overline{R}$有一个同态满射，R有零因子，$\overline{R}$可以没有零因子。

$R = \{(a, b) | a, b是整数\}$

加法：$(a_1, b_1) + (a_2, b_2) = (a_1 + a_2,\ b_1 + b_2)$

乘法：$(a_1, b_1)(a_2, b_2) = (a_1a_2, b_1b_2)$

R显然作成环。

$\overline{R}$是整数环Z。

ϕ： $(a, b) \longrightarrow a$

是R到$\overline{R}$的同态满射。

R有零因子：

$$(a,\ 0)(0,\ b) = (0,\ 0)$$

但$\overline{R}$没有零因子。

4. 环与真子环同构的例

例 $R[x]$是有单位元的交换环R上的一元多项式环。

令 $R[x^2] = \{所有a_0 + a_1x^2 + \cdots + a_nx^{2n} | a_i \in R\}$

显然 $R[x^2] \subset R[x]$

但 $x \overline{\in} R[x^2]$

否则

$$x = b_0 + b_1x^2 + \cdots + b_nx^{2n},\ b_0,\ b_1 \cdots b_n不全为0$$

则有 $b_0 - x + b_1x^2 + \cdots + b_nx^{2n} = 0$

这与x是R上未定元矛盾，所以$R[x^2]$是$R[x]$的真子集，至于x^2是R上未定元是显然的，且易见在

ϕ: $f(x) \to f(x^2)$ 之下，$R[x] \cong R[x^2]$

这就是说，$R[x^2]$是$R[x]$的真子环，且此真子环与$R[x]$同构。

5． 关于特征

例 在整数环Z与Z_p建立

$$\phi: \quad n \longrightarrow [n]$$

显然是Z到Z_p的一个同态满射。

而Z的特征是无限大，Z_p的特征是p。

§4 理 想

定义 环R的一个非空子集N叫做一个**左（右）理想子环**简称**左（右）理想**，假如

(i) $a, b \in N \Rightarrow a - b \in N$

(ii) $a \in N$，$r \in R \Rightarrow ra(ar) \in N$

假如N是R的左理想子环同时又是右理想子环，也就是说：

(i) $a, b \in N \Rightarrow a - b \in N$

(iii) $a \in N, r \in R \Rightarrow ra, ar \in N$

我们就把N叫做R的理想子环，简称理想

1． 偶数环是整数环Z的理想子环。

2． 是左理想子环而不是右理想子环的例

$$Z_{2\times2} = \left\{ \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix} \middle| a_{ij}\text{是整数} \right\}$$

$$N = \left\{ \begin{pmatrix} a & 0 \\ b & 0 \end{pmatrix} \middle| a,\ b\text{是整数} \right\}$$

易知N是$Z_{2\times 2}$的左理想子环而不是右理想子环。

3．是右理想子环而不是左理想子环的例

$$Z_{2\times 2}=\left\{\begin{pmatrix}a_{11} & a_{12}\\ a_{21} & a_{22}\end{pmatrix}\middle| a_{ij}\text{是整数}\right\}$$

$$N=\left\{\begin{pmatrix}a & b\\ 0 & 0\end{pmatrix}\middle| a,\ b\text{是整数}\right\}$$

易知N是$Z_{2\times 2}$的右理想子环，但不是左理想子环。

4．既不是左理想子环也不是右理想子环的例

$$Z_{2\times 2}=\left\{\begin{pmatrix}a_{11} & a_{12}\\ a_{21} & a_{22}\end{pmatrix}\middle| a_{ij}\text{是整数}\right\}$$

$$N=\left\{\begin{pmatrix}a & b\\ 0 & c\end{pmatrix}\middle| a,\ b,\ c\text{是整数}\right\}$$

N既不是$Z_{2\times 2}$的左理想子环也不是右理想子环。

5．我们知道"一个除环只有两个理想，就是零理想和单位理想"。

反之不真，即只有零理想和单位理想的环未必是除环。

例 $Q_{2\times 2}=\left\{\begin{pmatrix}a_{11} & a_{12}\\ a_{21} & a_{22}\end{pmatrix}\middle| a_{ij}\text{是有理数}\right\}$

我们说，$Q_{2\times 2}$只有零理想同单位理想。

设N是$Q_{2\times 2}$的一个理想，$N\neq O$

$$N\ni\begin{pmatrix}a_{11} & a_{12}\\ a_{21} & a_{22}\end{pmatrix}\neq\begin{pmatrix}0 & 0\\ 0 & 0\end{pmatrix}$$

不失一般性，假设$a_{11}\neq 0$。

那么

$$\begin{pmatrix}1 & 0\\ 0 & 0\end{pmatrix}\begin{pmatrix}a_{11} & a_{12}\\ a_{21} & a_{22}\end{pmatrix}\begin{pmatrix}1 & 0\\ 0 & 0\end{pmatrix}=\begin{pmatrix}a_{11} & 0\\ 0 & 0\end{pmatrix}\in N$$

$$\begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix}\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}=\begin{pmatrix} 0 & 0 \\ 0 & a_{11} \end{pmatrix}\in N$$

易知
$$\begin{pmatrix} a_{11} & 0 \\ 0 & a_{11} \end{pmatrix}\in N$$

$$\begin{pmatrix} a_{11}^{-1} & 0 \\ 0 & a_{11}^{-1} \end{pmatrix}\begin{pmatrix} a_{11} & 0 \\ 0 & a_{11} \end{pmatrix}=\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}\in N$$

所以 $N=Q_{2\times 2}$

但$Q_{2\times 2}$不是除环，因为

$$\begin{pmatrix} 1 & 2 \\ 2 & 4 \end{pmatrix}\text{没有逆。}$$

定义 $N=\{所有(x_1ay_1+\cdots+x_may_m+sa+at+na)\}$ 其中x_i，y_i，s，$t\in$环R，n是整数，把N叫做由a生成的**主理想**，用符号(a)表示；

当R是有单位元的交换环时，

$N=\{ra|r\in R\}$

当$N=\{所有s_1+s_2+\cdots+s_m|s_i\in(a_i)\}$

把N叫做由$a_1,a_2,\cdots,a_m$生成的理想，用符号$(a_1,a_2,\cdots,a_m)$表示。

6．主理想一定是理想，理想未必是主理想。

例 $Z[x]$是整数环Z上的一元多项式环，$(2,x)$是$Z[x]$的一个理想。

因为$Z[x]$是有单位元的交换环，

则 $(2,x)=\{所有2p_1(x)+xp_2(x)|p_i(x)\in Z[x]\}$

即 $(2,x)=\{所有2a_0+a_1x+\cdots+a_nx^n|a_i\in Z,n\geqslant 0\}$

我们说，$(2,x)$不是主理想。

假设$(2,x)=(p(x))$，就有

$2 \in (p(x))$，$x \in (p(x))$

即 $2 = q(x)p(x)$，$x = h(x)p(x)$

而 $2 = q(x)p(x) \Rightarrow p(x) = a$

$x = ah(x) \Rightarrow a = \pm 1$

这样，$\pm 1 = p(x) \in (2, x)$，± 1 显然写不成以下形式

$$2a_0 + a_1x + \cdots + a_nx^n$$

故矛盾。

$(2, x)$是$Q[x]$的一个主理想。（Q是有理数域）

7．对于环R的固定元a来说，$N = \{ra | r \in R\}$构成R的理想，但不一定有$N \ni a$。

例 R是偶数环，$N = \{所有r4 | r \in R\}$．易知 N 是 R 的理想。

但$4 \overline{\in} N$，这是因为R没有单位元，r始终不能取1。

这也就是说，N是理想，但不是由4生成的主理想。

定义 一个环R的而不等于R的理想 N 叫做一个**最大理想**．若除了R与N自己外，没有包含N的理想。

8．一个环的最大理想不一定只有一个。

例 Z是整数环，$N = (p)$，而p是素数。易知（p）是R最大理想。

意思是只要 p 是素数，（p）就是最大理想。如(2)，(3)，(5)…都是Z的最大理想。

注意：当p是非素数时，（p）不是整数环 Z 的最大理想。

当$p = 0$时，$(p) = 0$，$Z \supset (2) \supset (0)$

当$p = 1$时，$(p) = Z$

当$p = mn$（$m \neq 1$，$n \neq 1$），$Z \supset (m) \supset (p)$

9. F数域，$p(x)$是多项式环$F[x]$里的一个不可约多项式，则$(p(x))$是$F(x)$的最大理想。

10. $Z[x]$是整数环Z上一元多项式环，$Z[x]$的理想(x)不是$Z[x]$的最大理想，明显地有$(x)\subset(2, x)\subset Z[x]$，且$(x)\neq(2, x)$；$(2, x)\neq Z[x]$。

11. 一个无零因子的非交换环不一定能被一个除环包含。

例 参看：*A. Malcev, On the Immersion of an Algebraic Ring into a Field, Math Ann P.*113.1936.

§5 整环里的因子分解

1. 单位

定义 整环I的一个元ε叫做I的一个**单位**，假如ε是一个有逆元的元。

元b叫做元a的**相伴元**，假如b是a和一个单位ε的乘积：

$$b=\varepsilon a$$

我们说，单位元一定是单位，**但反之不真**。

例 整数环是整环I。$-1\in I$，而-1是单位，但不是单位元。

2. 唯一分解

定义 整环I的一个元p叫做一个**素元**，假如p既不是零元，也不是单位，并且p只有平凡因子。

定义 一个整环I的一个元a在I里有**唯一分解**，假如以下条件被满足：

(i) $a=p_1p_2\cdots p_r$ （p_i是I的素元）

（ii）若同时

$$a = q_1 q_2 \cdots q_s \qquad (q_i\text{是}I\text{的素元})$$

那么

$$r = s$$

并且把q_i的次序掉换一下，使得

$$q_i = \varepsilon_i p_i \qquad (\varepsilon_i\text{是}I\text{的单位})$$

1）既没有素元也没有可分解元的环是存在的。

例 任意域都是既没有素元也没有可分解元的环。

2）不能分解为素元乘积的环

例 1 $R = \{a_1 2^{x_1} + a_2 2^{x_2} + \cdots + a_n 2^{x_n}\}$

其中n是自然数，a_1，a_2，…，a_n是整数，x_1，x_2，…，x_n是非负的二进有理数，即形如$\frac{m}{2^k}$，此处m，k是非负整数。

形如

$a_1 2^{x_1} + a_2 2^{x_2} + \cdots + a_n 2^{x_n}$

的数的和、差、积仍为如是形状，此即说明R是环。

当 $n = 1$，$x_1 = 0$时，以上形式的数成为a_1，而a_1是任意整数，所以R包含所有整数，特别地含有单位元1。

数目2在R中可以分解为以下形状

$$2 = 2^{\frac{1}{2}} 2^{\frac{1}{2}} = 2^{\frac{1}{2}} 2^{\frac{1}{4}} 2^{\frac{1}{4}} = 2^{\frac{1}{2}} 2^{\frac{1}{4}} 2^{\frac{1}{8}} 2^{\frac{1}{8}} = \cdots$$

可以证明，数2以及形如$2^{\frac{1}{2^k}}$（k是非负整数）的数都不是R的单位。

因此，2在R中不能分解为素元的乘积。

例 2 设F为域，作

$$R=\{a_1x^{\alpha_1}+a_2x^{\alpha_2}+\cdots+a_nx^{\alpha_n}\mid a_1,\ a_2,\ \cdots,a_n\in F,$$
$$\alpha_1,\ \alpha_2,\cdots\alpha_n\text{是非负有理数}\}$$

在R中规定加法

$$f(x)+g(x)=(a_1x^{\alpha_1}+a_2x^{\alpha_2}+\cdots+a_nx^{\alpha_n})+$$
$$+(b_1x^{\alpha_1}+b_2x^{\alpha_2}+\cdots+b_nx^{\alpha_n})$$
$$=(a_1+b_1)x^{\alpha_1}+(a_2+b_2)x^{\alpha_2}+\cdots+$$
$$+(a_n+b_n)x^{\alpha_n}$$

在R中规定乘法

$$f(x)g(x)=(a_1x^{\alpha_1}+a_2x^{\alpha_2}+\cdots+a_nx^{\alpha_n})\times$$
$$\times(b_1x^{\beta_1}+b_2x^{\beta_1}+\cdots+b_mx^{\beta_m})$$
$$=\sum_{j=1}^{n}\sum_{k=1}^{m}a_jb_kx^{\alpha_j+\beta_k}$$

则R为一整环。

非零元x既不是单位也不是素元，然而

$$x=x^{\frac{1}{2}}x^{\frac{1}{2}}=x^{\frac{1}{2}}x^{\frac{1}{4}}x^{\frac{1}{4}}=x^{\frac{1}{2}}x^{\frac{1}{4}}x^{\frac{1}{8}}x^{\frac{1}{8}}=\cdots$$

$x^{\frac{1}{2}}$，$x^{\frac{1}{4}}$，$x^{\frac{1}{8}}$，…后者为前者的真因子，这说明x不能分解为有限个素元的乘积。

3）非唯一分解环

我们问，是不是整环I的既不等于零也不等于单位的元都有唯一分解？回答是未必。

例　$I=\{$所有$a+b\sqrt{-3}\mid a$，b是整数$\}$

I是整环。

（1）I的一个元ε是单位，当而且只当$|\varepsilon|^2=1$.（利用复数绝对值的概念）

（2）适合条件$|\alpha|^2=4$的I的元α一定是素元。

首先，既然$|\alpha|^2=4$，$\alpha\neq 0$，并由（1）α也不是单位，假定β是α的因子：

$$\beta=a+b\sqrt{-3}，\alpha=\beta\gamma$$

就有 $$4=|\beta|^2|\gamma|^2$$

不管a，b是什么整数，

$$|\beta|^2=a^2+3b^2\neq 2$$

因此 $|\beta|^2=1$ 或 4。

若是 $|\beta|^2=1$，由（1），β是单位。

若是 $|\beta|^2=4$，那么$|\gamma|^2=1$，γ是单位。

因而 $\beta=\gamma^{-1}\alpha$

β是α的相伴元，这样α只有平凡因子，α是素元。

现在看I的元4。

$$\begin{aligned}4&=2\cdot 2\\&=(1+\sqrt{-3})(1-\sqrt{-3})\end{aligned}\qquad (A)$$

因为$|2|^2=4$，$|1+\sqrt{-3}|^2=4$，$|1-\sqrt{-3}|^2=4$ 由（2），2，$1+\sqrt{-3}$，$1-\sqrt{-3}$都是I的素元，这就是说，(A)表示4在I里有两种分解，由(1)，$1+\sqrt{-3}$，$1-\sqrt{-3}$都不是2的相伴元，因而按定义以上两种分解不同。这样4在I里有两种不同的分解。

3. 最大公因子

定义 元c叫做a_1，$a_2,\cdots,a_n$的**公因子**，假如c同时能够整除a_1，$a_2,\cdots,a_n$。

元$a_1,a_2,\cdots,a_n$的一个公因子d叫做$a_1,a_2\cdots,a_n$的**最大公因子**，假如d能够被$a_1,a_2,\cdots,a_n$的每一个公因子c整除。

在整环里的两个元是不是一定有最大公因子？

例 $I=\{a+b\sqrt{5}\,|a，b是整数\}$

I是整环。

可以证明在I里$1-\sqrt{5}$和$3+\sqrt{5}$是相伴元，都不是单位；$1+\sqrt{5}$和$3-\sqrt{5}$是相伴元，都不是单位。明显地有

$$1+\sqrt{5}=(2+\sqrt{5})(3-\sqrt{5})$$

由于$a+b\sqrt{5}$是单位的充分与必要条件为$a^2-5b^2=\pm 1$。故可推断$2+\sqrt{5}$是单位。

$$4=2\cdot 2=(3+\sqrt{5})(3-\sqrt{5})$$

而2，$3+\sqrt{5}$，$3-\sqrt{5}$是素元，$3+\sqrt{5}$不是2的相伴元，这样，4在I里有两种不同的分解。

4和$2+2\sqrt{5}=2(1+\sqrt{5})$没有最大公因子。2和$1+\sqrt{5}$只是公因子而不是最大公因子。

4．唯一分解环、主理想环、欧氏环

定义 一个整环I叫做一个**唯一分解环**，假如I的每一个既不等于零又不是单位的元都有唯一分解。

定义 一个整环I叫做一个**主理想环**，假如I的每一个理想都是主理想。

定义 一个整环I叫做一个**欧氏环**，假如

(i) 有一个从I的非零元所作成的集合到$\geqslant 0$的整数集合的映射ϕ存在；

(ii) 给定了I的一个不等于零的元a，I的任何元b都可以写成

$$b=qa+\gamma \qquad (q,\ \gamma\in I)$$

的形式。这里或是$\gamma=0$或是$\phi(\gamma)<\phi(a)$。

我们知道：

一个主理想环I是一个唯一分解环；任何欧氏环I一定

是一个主理想环。但反之不真。即唯一分解环不一定是主理想环；而主理想环不一定是欧氏环。

例 1　Z 是整数环，那么 $Z[x]$是唯一分解环，但 $Z[x]$ 不是主理想环，这是因为：$Z[x]$ 的 理 想 $(2, x)$ 不是主理想。

例 2　I是唯一分解环，那么$I[x,y]$也是唯一分解环。

$$J=\{xf(x,y)+yg(x,y)\,|\,f(x,y),g(x,y)\in I[x,y]\}$$

则J是理想，但不是主理想。

若J为主理想，则有$h(x, y)$使

$$J=(h(x, y))$$

但$x,y\in J$，所以

$h(x,y)\,|\,x$，$h(x,y)\,|\,y\Rightarrow h(x,y)$为非零常数，

可是J不包含非零常数，故

$$J\neq(h(x,y))$$

例 3　一个主理想环不是欧氏环的例请参看：马士青（*Motzkin*），*The Euclidean algorithm*，*Bull. Amer. Math. Soc.* 55，*p.p.* 1142—1146，（1949）。